2023

Snohomish County Department of Human Services

Contractor Self-Assessment Monitoring Tool

SHSTJW

SNOHOMISH COUNTY | 3000 Rockefeller AVE, Everett WA 98201

Snohomish County
Department Of Human Services
3000 Rockefeller Ave, Everett WA 98201

Contract Name:
Contract #

Dear Contractor,

Snohomish County is encouraging and conducting contract monitoring and compliance of the Data Security Requirements Exhibit of your contract(s). Our goal in using this tool is to support your understanding of and compliance with your contract(s).

The tool is designed to be completed using a series of yes/no questions. Please answer all of the questions by checking the appropriate answer box. You may use the tab key on your keyboard to move from question to question and to the text fields. If an explanation is requested, please add a narrative response in the Contractor Explanation section which will expand to allow unlimited text. You may go back to a prior question by using the shift + tab keys on your keyboard.

Please return the completed monitoring tool to me no later than **2/28/2022**. Feel free to contact me if you have any questions about this Contractor Self-Assessment Monitoring Tool.

Sincerely,

Contracts Manager
Snohomish County Human Services /Developmental Disabilities
3000 Rockefeller MS305
Everett, WA 98201

Information that is exempt from disclosure to the public or other unauthorized persons under Chapter 42.56 RCW unauthorized persons under Chapter 42.56 RCW or other federal of state laws. Confidential information includes but is not limited to personal information. The contractor protects and maintains all Confidential Information against unauthorized use, access, disclosure modification or loss, including the following measures:		
45 CFR Part 164 – Security and Privacy Subpart C / Security Standards – 164.308 Administrative Safeguards		
(1)(i)(ii)(C) **Sanction policy (Required).** Do you have appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate?	☐ Yes ☐ No(Explain)	
(2) **Standard: Assigned security responsibility.** Have you Identified the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate?	☐ Yes ☐ No(Explain)	
(3) (i) **Standard: Workforce security.** Is security applied to ensure that all members of its workforce have appropriate access to electronic protected health information?	☐ Yes ☐ No(Explain)	
(4) (i) **Standard: Information access management.** (ii) **Implementation specifications:** (B) **Access authorization (Addressable).** Do you have policies and or procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism?	☐ Yes ☐ No	
(5) (i) **Standard: Security awareness and training.** Do you Implement a security awareness and training program for all members of its workforce (including management)?	☐ Yes ☐ No(Explain)	
(5) (i) (A) **Security reminders (Addressable).** Are periodic security updates applied?	☐ Yes ☐ No	
(5) (i) (B) **Protection from malicious software (Addressable).** Are systems for guarding against, detecting, and reporting malicious software in place?	☐ Yes ☐ No(Explain)	
(5) (i) (D) **Password management (Addressable).** Are the creating, changing, and safeguarding hardened passwords in place?	☐ Yes ☐ No(Explain)	
(6) (i) **Standard: Security incident procedures.** Do you meet the requirements to address security incidents?	☐ Yes ☐ No(Explain)	
(7) (i) **Standard: Contingency plan.** Do you have in place a plan for responding to an emergency or other occurrence(s)?	☐ Yes ☐ No(Explain)	
(8) **Standard: Evaluation.** Do you perform a periodic technical and nontechnical evaluations… under this rule?	☐ Yes ☐ No	

45 CFR Part 164 – Security and Privacy Subpart C / Security Standards – 164.310 Physical safeguards		
(a) (1) **Standard: Facility access controls.** Do you limit physical access to its electronic information systems, devices and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed?	☐ Yes ☐ No(Explain)	
(b) **Standard: Workstation use.** Are workstations, that can access electronic protected health information used in a way those functions are to be performed?	☐ Yes ☐ No(Explain)	
(c) **Standard: Workstation security.** Are physical safeguards in place for all workstations that access electronic protected health information, restrict access to authorized users?	☐ Yes ☐ No(Explain)	
(d) (1) **Standard: Device and media controls.** Is the use of hardware and electronic media (USB drives/CD) that contain electronic protected health information into and out of a facility, and the movement of these items within the facility secured?	☐ Yes ☐ No	
(d) (1) **Standard: Device and media controls.** (2) **Implementation specifications:** (i) **Disposal (Required).** Is the electronic protected health information, and/or the hardware (i.e., Copier) or electronic media on which it is stored disposed of securely?	☐ Yes ☐ No(Explain)	
(d) (1) **Standard: Device and media controls.** (2) **Implementation specifications:** (ii) **Media re-use (Required).** Is the removal of electronic protected health information from electronic media and or devices (i.e., cell phones, USB drives) before the media are made available for re-use?	☐ Yes ☐ No	
45 CFR Part 164 – Security and Privacy Subpart C / Security Standards – 164.312 Technical safeguards		
(a) (1) **Standard: Access control:** Is security implemented for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights?	☐ Yes ☐ No(Explain)	
(a) (1) **Standard: Access control. (2) Implementation specifications: (i) Unique user identification (Required).** Is a unique name and/or number for identifying and tracking user identity assigned?	☐ Yes ☐ No(Explain)	
(a) (1) Standard: Access control. (2) Implementation specifications: (ii) Emergency access procedure (Required). Is the ability for obtaining necessary electronic protected health information during an emergency in place?	☐ Yes ☐ No(Explain)	

(a) (1) Standard: Access control. (2) Implementation specifications: (iii) **Automatic logoff (Addressable).** Do the computers/devices terminate an electronic session after a predetermined time of inactivity?	☐ Yes (Explain) ☐ No	
(a) (1) Standard: Access control. (2) Implementation specifications: (iv) **Encryption and decryption (Addressable).** Is a mechanism to encrypt and decrypt (i.e., data at rest) electronic protected health information in place?	☐ Yes ☐ No (Explain)	
(d) **Standard: Person or entity authentication.** Is the verification that of a person or entity seeking access to electronic protected health information is the one claimed, implemented?	☐ Yes ☐ No (Explain)	
(e) (1) **Standard: Transmission security.** Are technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network in place?	☐ Yes ☐ No	
(e) (1) **Standard: Transmission security.** (ii) **Encryption (Addressable).** Is a mechanism to encrypt (i.e., in transit) electronic protected health information whenever deemed appropriate?	☐ Yes (Explain) ☐ No	

I hereby declare that the information I have given on this form is true, correct and complete to the best of my knowledge.

Signature	Printed Name
Date	Title
Phone Number	Email Address

Nearly any encryption software will need to be configured to provide the appropriate protection, minimum encryption key length of at least 256 bits for symmetric keys or 2048 bits for asymmetric keys. Snohomish County business partners are required by contracts to protect confidential and sensitive County data by applying encryption on computers and data storage devices where County data is stored. It is up to the business partner to determine the product that will meet HIPAA requirements prior to purchasing and/or using encryption products. Snohomish County does not have the resources to provide support to business partners in meeting this requirement.

NOTE: Windows 10, 11, Server 2016 and above versions come with Bit locker encryption at no additional charge. Full hard disk encryption is recommended over folder encryption. Full hard disk encryption provides the most protection as staff can store data anywhere on their device and it will be encrypted, whereas folder encryption will depend on the user to consistently store data only to the folder or portion of the drive that is encrypted. This leaves room for user error.

Source Link: https://www.hhs.gov/hipaa/for-professionals/security/index.html

Reviewed by Program Staff

Signature	Printed Name
Date	Title

Reviewed by Snohomish County Network Administrator

Signature	Printed Name
Date	Title

Subpart C — Security Standards for the Protection of Electronic Protected Health Information

HIPAA §164.308 Administrative safeguards.

(a) A covered entity or business associate must, in accordance with §164.306:

(1) (i) **Standard: Security management process.** Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) **Implementation specifications:**

(A) **Risk analysis (Required).** Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

(B) **Risk management (Required).** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).

(C) **Sanction policy (Required).** Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

(D) **Information system activity review (Required).** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

(2) **Standard: Assigned security responsibility.** Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

(3) (i) **Standard: Workforce security.** Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

(ii) **Implementation specifications:**

(A) **Authorization and/or supervision (Addressable).** Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

(B) **Workforce clearance procedure (Addressable).** Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

(C) **Termination procedures (Addressable).** Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

(4) (i) **Standard: Information access management.** Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

(ii) **Implementation specifications:**

(A) **Isolating health care clearinghouse functions (Required).** If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

(B) **Access authorization (Addressable).** Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

(C) **Access establishment and modification (Addressable).** Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

(5) (i) **Standard: Security awareness and training.** Implement a security awareness and training program for all members of its workforce (including management).

(ii) **Implementation specifications. Implement:**

(A) **Security reminders (Addressable).** Periodic security updates.

(B) **Protection from malicious software (Addressable).** Procedures for guarding against, detecting, and reporting malicious software.

(C) **Log-in monitoring (Addressable).** Procedures for monitoring log-in attempts and reporting discrepancies.

(D) **Password management (Addressable).** Procedures for creating, changing, and safeguarding passwords.

(6) (i) **Standard: Security incident procedures.** Implement policies and procedures to address security incidents.

(ii) **Implementation specification: Response and reporting (Required).** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

(7) (i) **Standard: Contingency plan.** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) **Implementation specifications:**

(A) **Data backup plan (Required).** Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) **Disaster recovery plan (Required).** Establish (and implement as needed) procedures to restore any loss of data.

(C) **Emergency mode operation plan (Required).** Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

(D) **Testing and revision procedures (Addressable).** Implement procedures for periodic testing and revision of contingency plans.

(E) **Applications and data criticality analysis (Addressable).** Assess the relative criticality of specific applications and data in support of other contingency plan components.

(8) **Standard: Evaluation.** Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.

(b) (1) **Business associate contracts and other arrangements.** A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a), that the subcontractor will appropriately safeguard the information.

(3) **Implementation specifications: Written contract or other arrangement (Required).** Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).

HIPAA 164.310 Physical safeguards.

A covered entity or business associate must, in accordance with §164.306:

(a) (1) **Standard: Facility access controls.** Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

(2) **Implementation specifications:**

(i) **Contingency operations (Addressable).** Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

(ii) **Facility security plan (Addressable).** Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

(iii) **Access control and validation procedures (Addressable).** Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

(iv) **Maintenance records (Addressable).** Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

(b) **Standard: Workstation use.** Implement policies and procedures that specify the proper functions to be performed, the way those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

(c) **Standard: Workstation security.** Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

(d) (1) **Standard: Device and media controls.** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

(2) **Implementation specifications:**

(i) **Disposal (Required).** Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

(ii) **Media re-use (Required).** Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

(iii) **Accountability (Addressable).** Maintain a record of the movements of hardware and electronic media and any person responsible, therefore.

(iv) **Data backup and storage (Addressable).** Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

HIPAA §164.312 Technical safeguards.

A covered entity or business associate must, in accordance with §164.306:

(a) (1) **Standard: Access control.** Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).

(2) **Implementation specifications:**

(i) **Unique user identification (Required).** Assign a unique name and/or number for identifying and tracking user identity.

(ii) **Emergency access procedure (Required).** Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

(iii) **Automatic logoff (Addressable).** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

(iv) **Encryption and decryption (Addressable).** Implement a mechanism to encrypt and decrypt electronic protected health information.

(b) **Standard: Audit controls.** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

(c) (1) **Standard: Integrity.** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

(2) **Implementation specification: Mechanism to authenticate electronic protected health information (Addressable).** Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

(d) **Standard: Person or entity authentication.** Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

(e) (1) **Standard: Transmission security.** Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

(2) **Implementation specifications:**

(i) **Integrity controls (Addressable).** Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

(ii) **Encryption (Addressable).** Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.