|  |
| --- |
| Instructions: These Security Rule Policies and Procedures must be adopted if the plan has any electronic protected health information. |
| **[Insert Health Plan Name] HIPAA Security Policies and Procedures (Required)** |

| **Standard/Implementation Specification** | **Policy/Procedure** |
| --- | --- |
| 1. **Risk Analysis/Risk Management**   Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the health plan.  Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. | **a. Individuals with ePHI Access.** The following individuals have access to electronic protected health information (“ePHI”): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.  **b. Routine Transmission Risk.**  The risk associated with routine transmission of ePHI is:  i. Confidentiality Risk 🞎 Low 🞎 Medium 🞎 High  Explanation of analysis: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.  ii. Integrity Risk 🞎 Low 🞎 Medium 🞎 High  Explanation of Analysis: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.  iii. Availability Risk 🞎 Low 🞎 Medium 🞎 High  Explanation of analysis: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **c. Routine Storage Risk.** The risk associated with routine storage of ePHI is:  i. Confidentiality Risk 🞎 Low 🞎 Medium 🞎 High  Explanation of analysis:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.  ii. Integrity Risk 🞎 Low 🞎 Medium 🞎 High  Explanation of analysis:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.  iii. Availability Risk 🞎 Low 🞎 Medium 🞎 High  Explanation of analysis:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **d. Non-Routine Transmission and Storage.** Transmission and storage of ePHI in a manner other than that identified above will be considered on a case-by-case basis by the Security Official.  **e. Additional Risk Analysis.** The plan will conduct an additional risk analysis 🞎 as reasonably determined by the Security Official 🞎 every 3 years 🞎 whenever there is a significant change in the plan's information technology environment or 🞎 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Sanction Policy**   Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures. | It is the policy of the health plan that its workforce [including employees of the plan sponsor who have access to ePHI] [Include if applicable; typically will apply to a single employer health plan] shall comply with the health plan's policies and procedures relating to the security of ePHI. Appropriate disciplinary procedures, up to and including termination of employment, will be imposed upon workforce members violating this policy. |
| 1. **Information System Activity Review**   Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | **a. ePHI in Physical Form.** ePHI in physical form (such as storage on a disk, CD-ROM or DVD) is located at the following locations: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.  **b. ePHI in Electronic Form.** ePHI in electronic form (such as storage on a computer's hard drive) is located at the following locations: .  **c. Procedure for Determining Access.** The health plan establishes the following procedure for determining whether an individual has accessed this ePHI stored in electronic form: [Describe procedure.For example, the health plan may have software that can track which computer user has accessed files containing ePHI]  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.  **d. Conducting of Review.** The Security Official will conduct an information system activity review every \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [Insert reasonable period of time. For example, "3 months" or "12 months".].  The Security Official shall use the information gathered in the review to determine whether ePHI was accessed by an internal user, who accessed the information and whether the access was proper. |
| 1. **Security Official Designation**   Identify the security official responsible for the development and implementation of HIPAA Security Rule policies and procedures. | Our health plan’s Security Official is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.  The Security Official will be responsible for developing and implementing polices and procedures to ensure the confidentiality, integrity and availability of all ePHI created, received, maintained or transmitted by the health plan.  Unless otherwise specified in any policy and procedure, the Security Official shall: (1) take all actions required of the health plan to comply with the Security Rule of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"); (2) have authority and responsibility to adopt a HIPAA Security Rule policy and / or procedure and complete any related forms; (3) have authority to modify a HIPAA Security Rule policy and/or procedure and any related forms; (4) have responsibility to retain all policies, procedures, forms, documents and training materials as required by the HIPAA Security Rule; and (5) periodically review and update all relevant policies, procedures, forms, documents and training materials as needed, in response to environmental or operational changes affecting the security of ePHI. |
| 1. **Response and Reporting**   Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the plan; and document security incidents and their outcomes. | The health plan will:  • Identify and respond to suspected or known security incidents involving ePHI;  • Mitigate, to the extent practicable, harmful effects of security incidents known to the health plan; and  • Document security incidents and their outcomes.  All such actions shall be taken by the Security Official as promptly as possible after learning of a security incident or suspected security incident. The Security Official shall determine the risk associated with the security incident and take an appropriate action based on the facts and circumstances of the situation. |
| 1. **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 ePHI. | **a. Data Backup Plan.** The health plan will have a data backup plan to help secure ePHI. The backup plan will be created and overseen by the Security Official and implemented as soon as reasonably possible. The backup plan will be designed to create and maintain retrievable exact copies of ePHI. Describe relevant details (e.g., data to be included, frequency, who conducts it): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.  **b. Disaster Recovery Plan.** The health plan will have a disaster recovery plan. The disaster recovery plan will be designed to restore any loss of relevant ePHI. The Security Official shall take all necessary steps in the event of a disaster recovery, including, e.g., assessing the damage, loss of data and contacting of third party vendors to assist. Describe plan: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.  **c. Emergency Mode Operation Plan.** The health plan will establish and implement an emergency mode operation plan. The emergency mode operation plan will be designed to enable the health plan to continue critical business processes for protecting the security of ePHI while operating in emergency mode. Describe the emergency mode operation plan (e.g., reliance on third party administrator with separate data): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  . |
| 1. **Evaluation**   Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under the Security Rule and subsequently, in response to environmental or operational changes affecting the security of ePHI that establishes the extent to which the plan's security policies and procedures meet the requirements of the HIPAA Security Rule. | The Security Official or a designee shall periodically evaluate these policies and procedures to determine compliance with the HIPAA Security Rule. Such evaluation shall be made: [Describe – e.g., "once per year" or "as needed"] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Business Associate Contracts**   Permit a business associate to create, receive, maintain, or transmit ePHI on the Plan's behalf only if we obtain satisfactory assurances that the business associate will appropriately safeguard the information. | Use Form 1, Business Associate Agreement (or another, approved agreement) to ensure compliance with this rule. |
| 1. **Workstation Use**   Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI. | **a. General Workstation Security.** The Security Official will determine which functions are appropriate for particular workstations. For example, it may not be appropriate to have a receptionist desk (which the public can view) accessing ePHI. Considering these factors, the Security Official implements the following procedure and physical safeguards: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.  **b. Protection of Integrity and Availability of ePHI.** The health plan will reasonably protect the integrity and availability of ePHI. The health plan will do so by using all reasonable means, including: [Describe—e.g., requiring password-protected screen savers after a certain time period; requiring log off of users at the end of the day, etc.] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.  **c. Physical Attributes of Surroundings.** The physical attributes of workstation surroundings will be considered and the following protections implemented: [Describe—e.g., positioning monitors so ePHI cannot be viewed by unauthorized individuals]: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Workstation Security**   Implement physical safeguards for all workstations that access ePHI to restrict access to authorized users. | The Security Official will identify which workstations could have access to ePHI and implement the following physical security measures: [Describe—e.g., anti-theft devices on workstations, keeping an inventory of workstations, etc.] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Disposal and Media Re-Use**   • Disposal - Policies and procedures to address the final disposition of ePHI and/or the hardware or electronic media on which it is stored. All devices which store ePHI should be considered, including photocopiers, facsimile machines and other office machines which may store ePHI.  • Media re-use - Procedures for removal of ePHI from electronic media before the media are made available for re-use. | **a. Training.** The Security Official shall train all workforce members that, when disposing of hardware and other electronic media containing ePHI, the hardware or media must be (a) sanitized so no ePHI is accessible; or (b) destroyed or altered so that no ePHI is accessible. If needed, the following additional steps will be taken to implement this: [Describe any—e.g., placing a small sticker on hardware reminding of need for destruction in accordance with HIPAA] .  **b. Media to be Re-Used.** If media will be re-used, identify such media \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.  **c. Sanitizing of Media.** State how such media will be sanitized prior to re-use: [Describe hardware or software used to sanitize] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Unique User Identification and Emergency Access Procedure**   • Unique user identification - Assign a unique name and/or number for identifying and tracking user identity.  • Emergency access procedure - Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency. | It is the policy of the health plan that it will have a procedure for (a) assigning a unique name and/or number for identifying and tracking user identity; and (b) obtaining necessary ePHI during an emergency.  **a. Review of Current Software.** The Security Official will determine whether the health plan's current software automatically assigns a unique name and / or number for identifying and tracking user identity.  **b. Action Based on Review.** The Security Official believes that the health plan's current software is 🞎 adequate and satisfies this requirement 🞎 not adequate. If current software is not adequate, the Security Official will remedy this by: [Describe – e.g., purchasing new software] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.  **c. Providing Temporary, Emergency Access.** The Security Official will 🞎 use existing software 🞎 modify existing software to allow temporary access to ePHI to an approved user during an emergency. |
| 1. **Audit Controls**   Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. | **a. Identification of Audit Control Features.** The Security Official will identify audit control features of the health plan's existing software that can help determine which users have accessed ePHI. This is as follows: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.  **b. Additional Controls.** If such controls are not sufficient, the Security Official will implement additional controls, as described here: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Person or Entity Authentication**   Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed. | The health plan will verify authentication by doing the following: [Describe—e.g., using passwords or PIN numbers] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Maintenance**   The Security Rule Policies and Procedures must be periodically reviewed and updated. | We will periodically review and update our Required and Addressable Security Rule Policies and Procedures as needed to continue to provide reasonable and appropriate protection of ePHI in response to environmental or operational changes affecting the security of ePHI. We will update such Policies and Procedures to reflect these items and make the updated (and current) documentation available to those persons responsible for implementing our procedures to which the documentation pertains. |

**Adoption of Policies and Procedures**. The undersigned represents that he or she has authority to adopt these policies and procedures on behalf of the above-named health plan.

Adopted this \_\_\_\_ day of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 20\_\_.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title

QB\21427355.1