|  |
| --- |
| Instructions: These items are "addressable" HIPAA Security Rule considerations. They must be completed if the plan has any electronic protected health information. |
| **[Insert Health Plan Name] HIPAA Security Policies and Procedures (Addressable)** |
| Note: For each Implementation Specification, consider the risk if it is not implemented, the cost of implementing, the benefit of implementing and the feasibility of implementing the Implementation Specification. For each Implementation Specification that is not implemented due to one of these factors (e.g., it is not feasible), complete Form 15, Alternative Measures. |

| **Standard /** **Implementation Specification** | **Policy/Procedure** |
| --- | --- |
| 1. **Authorization and/or Supervision**

Procedures for the authorization and/or supervision of workforce members who work with electronic protected health information ("ePHI") or in locations where it might be accessed. | The Security Official 🞎 will 🞎 will not pre-authorize or pre-screen workforce members a being trustworthy to obtain ePHI and being able to follow the health plan's policies and procedures regarding ePHI.Comment here as needed:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Workforce Clearance Procedure**

Procedures to determine that the access of a workforce member to ePHI is appropriate. | It is the policy of the health plan that the Security Official 🞎 will 🞎 will not determine whether a particular workforce member may access all or some ePHI. The Security Official 🞎 will 🞎 will not require completion of a background investigation on 🞎 all 🞎 some employees who handle ePHI.If "some" is selected, explain the criteria for background investigation here: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.Comment here as needed:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Reinvestigation of Workforce Clearance Procedure (suggested in HHS guidance; presumably addressable).**

See Centers for Medicare & Medicaid Services (CMS) – Office of E-Health Standards and Services (OESS) – Reviews 2008 (available at <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/cmscompliancerev08.pdf>).  | It is the policy of the health plan that the Security Official 🞎 will 🞎 will not reinvestigate whether a particular workforce member may access all or some ePHI.Comment here as needed:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Termination Procedures**

Procedures for terminating access to ePHI when the employment of a workforce member ends or as required by determinations made under the workforce clearance procedure, above. | The health plan 🞎 will 🞎 will not adopt a policy and procedure regarding the termination of employment of a workforce member who had access to ePHI. If "will" is selected it is the policy of the health plan that the health plan will take reasonable and appropriate steps to ensure that ePHI is not accessed by workforce members who have terminated employment. The Security Official shall take all necessary steps to ensure this policy is implemented, including: [Describe steps—e.g., requiring return of keys or key cards, requiring return of laptops with ePHI] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Comment here as needed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Access Authorization**

Policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism. | The health plan 🞎 will 🞎 will not have a policy and procedure to determine whether a workforce member may access ePHI. If selected, the Security Official will: [Describe – e.g., make the determination on a case-by-case basis] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.Comment here as needed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Access Establishment and Modification.**

Policies and procedures that establish, document, review and modify a user's right of access to a workstation, transaction, program or process. | The health plan 🞎 will 🞎 will not take reasonable and appropriate steps to ensure that only approved workforce members or others may have access to ePHI. If selected, the Security Official will grant or modify such access when the Security Official deems reasonable and appropriate. The Security Official shall take all necessary steps to ensure this policy is implemented, including: [Describe – e.g., providing passwords to only approved individuals; screensavers or passwords on computers; placing ePHI in restricted files] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.Comment here as needed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |

|  |  |
| --- | --- |
| 1. **Security Reminders**
 | The Security Official 🞎 will 🞎 will not issue periodic security reminders.Comment here as needed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Protection From Malicious Software**

Guarding against, detecting and reporting malicious software. | The Security Official 🞎 will 🞎 will not ensure the plan has sufficient protection from malicious software. If selected, the health plan will examine its vulnerability to particular, known malicious software and will: [Describe – e.g., use certain software to protect against such risks] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.If selected, the Security Official will take steps to ensure that he or she maintains current knowledge about malicious software.Comment here as needed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Log-in Monitoring**

Monitoring log-in attempts and reporting discrepancies. | The health plan’s policy is to monitor log-in attempts of users. If the log-in is successful on the first attempt 🞎 no log-in report will be generated 🞎 a log-in report will be generated. If the log-in is unsuccessful a log-in report will be generated 🞎 every time 🞎 after \_\_\_\_\_ [*Insert number*] consecutive attempts. The log-in report will be promptly reviewed by the Security Official and investigated as reasonable and appropriate.Comment here as needed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Password Management**

Creating, changing and safeguarding passwords. | The health plan 🞎 will 🞎 will not take appropriate steps to ensure the use and confidentiality of passwords. If selected, the health plan implements the following requirements regarding passwords: [Describe - e.g., passwords must be of a certain length; will be changed every 90 days, etc.] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.Comment here as needed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |

|  |  |
| --- | --- |
| 1. **Testing and Revision Procedures**

Implement procedures for periodic testing and revision of contingency plans. | It 🞎 is 🞎 is not the policy of the health plan to establish procedures for the periodic testing and revision of its contingency plan. This testing will be done as follows: [Describe – e.g., done "every year" and "by Security Official"] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Comment here as needed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Applications and Data Criticality Analysis**

Assess the relative criticality of specific applications and data in support of other contingency plan components. | It 🞎 is 🞎 is not the policy of the health plan to conduct an applications and data criticality analysis. If selected, it is conducted by: [Describe – e.g., identify who performs it and when]: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.Comment here as needed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Contingency Operations**

Procedures to allow access to the health plan’s facility to help restore data lost in an emergency, considering the disaster recovery plan and emergency mode operations plan. | The health plan 🞎 will 🞎 will not have a policy to allow reasonable facility access to authorized personnel to restore data lost due to an emergency. If selected, this policy will work in conjunction with any disaster recovery plan and emergency mode operations plan. The Security Official will, if reasonable and appropriate, accompany the workforce member or third party vendor when they work to recover the lost data. The Security Official will consider whether any third parties will be considered business associates under HIPAA. Comment here as needed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Facility Security Plan**

Policies and procedures to safeguard the facility and its equipment from unauthorized physical access, tampering and theft. | The health plan 🞎will 🞎 will not have a policy to safeguard its facility and equipment therein from unauthorized physical access, tampering and theft. The health plan will: [Describe – e.g., require security badges, etc.] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.Comment here as needed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Access Control and Validation Procedures**

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. | The health plan 🞎 will 🞎 will not have a policy to control and validate a person’s access to its facilities, based on the person’s role or function. This includes visitor control and control of access to software programs for testing and revision. The health plan will: [Describe – e.g., require visitors to sign in; provide identification badges, etc.] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.Comment here as needed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Maintenance Records**

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). | The health plan 🞎 will 🞎 will not have a policy to document repairs and modifications to the physical components of a facility which are related to security (including but not limited to hardware, walls, doors and locks). If selected, the health plan will: [Describe – e.g., record all maintenance activity] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.Comment here as needed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Accountability**

Consider whether to maintain a record of hardware and electronic media and any person responsible for those items. | The health plan 🞎 will 🞎 will not have a policy to maintain a record of hardware and electronic media and any person responsible for those items. If selected, the Security Official will create and maintain this list.Comment here as needed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Data Backup and Storage**

Consider whether the health plan should be able to create a retrievable, exact copy of ePHI, when needed, before movement of equipment. | The health plan 🞎 will 🞎 will not have a policy to take the necessary steps to be able to create a retrievable, exact copy of ePHI, when needed, before movement of equipment. Comment here as needed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |

|  |  |
| --- | --- |
| 1. **Automatic Logoff**

Consider whether to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. | The health plan 🞎 will 🞎 will not have a policy to terminate an electronic session after \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.[Describe time period – e.g., "5 minutes" or "30 minutes"].Comment here as needed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Encryption and Decryption**

Consider whether to implement a mechanism to encrypt and decrypt ePHI (generally, when stored in the health plan's electronic communications system; see below for encryption as part of transmission). Note that some HHS guidance states that while encryption is addressable, changes in the technology industry have created an "environment where encryption may not be optional under the mantra of reasonable and appropriate." See HIPAA Compliance Review Analysis and Summary of Results – Centers for Medicare & Medicaid Services (CMS) – Office of E-Health Standards and Services (OESS). Also, a January 2013 regulation discusses unencrypted emails in connection with an individual's request to obtain a copy of protected health information. The regulation states that the plan is permitted to send individuals unencrypted emails if the plan has advised the individual of the risk and the individual still prefers the unencrypted email. (78 Fed. Reg. at 5634 (Jan. 25, 2013)) | The health plan 🞎 will 🞎 will not have a mechanism to encrypt and decrypt ePHI while stored. If selected, the plan will: [Describe – e.g., use current software] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.Comment here as needed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Mechanism to Authenticate Electronic Protected Health Information**

Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner. | The health plan 🞎 will 🞎 will not implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner. The health plan will do this by: [Describe – e.g., using current software and its built-in features] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.Comment here as needed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Integrity Controls**

Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until properly disposed. | The health plan 🞎 will 🞎 will not have a policy to implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until properly disposed. This will be accomplished by: [Describe – e.g., use current software] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.Comment here as needed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| 1. **Encryption (as part of transmission security of ePHI)**

Implement a mechanism to encrypt ePHI whenever deemed appropriate. | The health plan 🞎 will 🞎 will not have a policy to encrypt ePHI when it travels over an electronic communications network. If selected, this will be accomplished by: [Describe—e.g., transmission to a business associate, which occurs automatically using current software] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.Comment here as needed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |

**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\21427354.1