****

Veterans Health Administration (VHA)

Privacy and Security Checklist for Reviewing Mobile Applications

**Developer fills out page 1 and 4, Privacy fills out page 2, and Security fills out page 3.**

 **Developer Contact Information**

|  |  |  |
| --- | --- | --- |
| **Developer Name** | **VA E-Mail Address** | **Phone Number** |
| **Office and Routing Symbol** | **Web and Mobile Solutions** | **Fax Number** |

**Mobile Application Information**

|  |  |  |
| --- | --- | --- |
| Name of Mobile Application  | Date of Development  | **Web address where mobile application can be viewed:**  |
| Description of Mobile Application  |
| Intended Audience (User) for Mobile Application: [ ]  Veteran [ ] Caregiver [ ] Provider [ ] Public |
| Does User enter information or data into the Mobile Application? [ ]  Yes [ ]  No [ ]  N/A | Does Mobile Application store information or data entered by the User? [ ]  Yes [ ]  No [ ]  N/A | Does Mobile Application transmit/push data entered to VA? [ ]  Yes [ ]  No [ ]  N/A |
| If the answer to any of the questions above are “yes” then describe what information or data is entered or transmitted to VA: |
| Does Mobile Application pull data from a VA Database? [ ]  Yes [ ]  No [ ]  N/A | Does the Mobile Application store information or data pulled from a VA Database? [ ]  Yes [ ]  No [ ]  N/A  |  |
| If the answer to any of the questions above are “yes” then describe what information or data is pulled from a VA database: |
| Type of Mobile Application Section must be filled out by the Developer prior to the Mobile Application submitted for Privacy and Security Review: |
| **Type of Mobile Application**: (More than One Box may be Checked)[ ]  Mobile Application Stores/Transmits Veteran Specific Data Entered by VA Provider [ ]  Mobile Application Pulls Data from VA Database and Stores It [ ]  Mobile Application Pulls Data from VA Database But Does Not Store It [ ]  Mobile Application Stores Data Entered by the Veteran Only [ ]  Mobile Application Allows for Entry and Transmission of Data Entered by the Veteran to VA [ ]  Informational Mobile Application – No Data Pulled from VA and No Data Transmitted/Pushed to VA NOTE: If **informational Mobile Application** box is checked, no Privacy Review or Security Review is required and checklist only needs to be signed by Developer. If any of the other boxes are checked a Privacy and Security Review must be completed.  |
| **Check any of the following HIPAA identifiers that may be stored, entered, displayed or collected on the Mobile Application: If nothing is applicable check the box below** |
| **[ ] Names** | **[ ]  Telephone Numbers** | **[ ]  Device Identifiers and Serial Numbers** |
| **[ ]  E-mail Addresses** | **[ ]  Fax Numbers** | **[ ]  URLs (Universal Resource Locator)** |
| **[ ]  SSN or Medical Record Number**  | **[ ]  IP Addresses (Internet Protocol)** | **[ ]  Account Numbers** |
| **[ ]  Health Plan Beneficiary Number** | **[ ]  Certificate or License Numbers** | **[ ]  No Identifiers are being stored, entered, displayed or collected on the device**  |
| **[ ]  Other Identifier (Provide Description):** |

**Privacy and Confidentiality Requirements**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Section to be completed by the Appropriate Privacy Office** | **Met**  | **Not Met** | **N/A** | **Comments** |
| **1** | **VA data pulled from VA database is a disclosure to the Veteran and stored on Veteran’s device. EULA used covers that Veteran owns the data now stored on the device.**  |  |  |  |  |
| **2** | **VA data pulled from VA database is a disclosure to the Veteran but is not stored on the Veteran’s device. EULA used covers the fact that the Veteran is not being provided a copy but is only being given access to the data through the device.** |  |  |  |  |
| **3** | **Veteran self-entered data is not transmitted to VA but is securely stored on the device as determined by HCSR.** |  |  |  |  |
| **4** | **Veteran self-entered data transmitted to VA is covered by a Privacy Act system of records. EULA used covers the VA will receive the data entered by the Veteran on the device.** |  |  |  |  |
| **5** | **VA Provider entered data transmitted to VA is covered by a Privacy Act system of records.** |  |  |  |  |
| **6** | **VA data pulled from VA database and displayed to VA provider in performance of official duties is not stored on device.**  |  |  |  |  |
| **7** | **VA data pulled from VA database displayed to and modified by VA Provider in performance of their official duties is transmitted to VA for inclusion in the appropriate Federal Record or in a Privacy Act System of Records.** |  |  |  |  |
| **8** | **Account Information is not transferred to the mobile application.**  |  |  |  |  |

**Privacy Officer’s Signature Section**

|  |
| --- |
| **I have reviewed the Mobile Application and attest that it meets applicable privacy requirements.****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **Signature or E-signature of Privacy Office Representative Date** |

**Security Requirements**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Section To Be Completed by Appropriate Security Official** | Met  | Not Met | N/A | Comments |
| **9** | **Access Control: Access to any PHI/PII is restricted by password, PIN, or other appropriate access control mechanism.**  |  |  |  |  |
| **10** | **Data Storage: All stored PHI/PII will be encrypted with VA-approved encryption that is FIPS 140-2 validated.**  |  |  |  |  |
| **11** | **Data Transmission: All PHI/PII transmitted to or from VA will be encrypted with VA-approved encryption that is FIPS 140-2 validated.**  |  |  |  |  |
| **12** | **Data Removal: If PHI/PII is stored on a device a mechanism must be in place to remove all stored PHI/PII.** |  |  |  |  |

**Heath Care Security Requirements Signature Section**

|  |
| --- |
| **I have reviewed the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Mobile Application and attest that it meets applicable security requirements.****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_****Signature or E-signature of Health Care Security Requirements representative Date**  |
| **Developer Signature:** **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_****Final Signature or E-signature of Developer Date**  |