Step 1: Complete and return required documentation to PSYCKES Team

a) Provider completes "PSYCKES Access Online Contact Form" survey:
https://www.surveymonkey.com/r/PSYCKES_Access_Contact_Form

b) Provider CEO (or another person who is legally authorized to bind the organization to the contractual terms) signs the Office of Mental Health (OMH) PSYCKES Confidentiality Agreement in which the organization acknowledges that PSYCKES provides access to Medicaid claims data and protected health information and agrees to comply with all New York State and Federal privacy laws and regulations. Agreements will be countersigned by the Medical Informatics Director in the OMH Office of Population Health and Evaluation.
   - Scan signed copy and email to psyckes-help@omh.ny.gov

If organization already has a Security Manager to create PSYCKES users, skip to step 4

Step 2: Complete registration in OMH Security Management System (SMS)

Access to secure OMH applications, including PSYCKES, is managed through an online SMS (for more information, see https://www.omh.ny.gov/omhweb/sms/).

a) OMH emails instructions to the CEO on how to electronically sign a Confidentiality and Non-Disclosure Agreement (CNDA). (This is separate from the PSYCKES-specific Confidentiality Agreement referenced in step 1b above.)
b) The CEO follows instructions provided in the email to electronically sign the CNDA.

Step 3: Designate one or more Security Manager

a) OMH emails the CEO with information and self-registration link needed to assign one or more SMS Security Managers.
b) CEO forwards email to person(s) who are to become Security Manager(s).
c) Staff follow instructions in email for online self-registration process as Security Manager.
d) OMH sends the Security Manager an email notification and token information (if needed, staff with existing OMH tokens will be able to use the same token).
e) The Security Manager follows token instructions and logs into SMS.

CEO/ED should save the email described in step 3a in case additional security mangers are needed in the future. If this email gets misplaced, contact OMH Helpdesk at heathhelp@its.ny.gov to request that the SMS self-registration email be resent.

Step 4: Security Manager enrolls PSYCKES users

a) Provider determines staff requiring PSYCKES access.
b) Security Manager creates an account in SMS (if needed; staff with existing OMH accounts in SMS and existing tokens will be able to use the same user ID and token). The Security Manager will need the following information to create accounts in SMS:
   i. First and Last Name
   ii. Title
   iii. E-mail Address (note: correct email of user is critical because User ID, token information and all PSYCKES application communications are emailed to users)
   iv. Work Phone Number
   v. Token Type Needed: Either mobile-based "soft" token or physical "hard" token
c) Once the user account is created, the Security Manager uses SMS to grant access to PSYCKES by selecting the "PSYCKES-Medicaid" access option check box.
d) After the Security Manager grants access, OMH Security will directly email the user with their specific token instructions:
   - For users whose Security Manager selected "soft token" access, they will receive an email from OMH Security containing a link to the Self-Service Console as well as a User ID and password to login to the Console. Within the Console, users will submit a request for their mobile token and specify which mobile device they have (iOS, Android, etc.). After their mobile token is issued, they will use the Console to activate their token.
   - For users whose Security Manager selected "hard token" access, they will first need to be provided the hard token from their Security Manager, as hard tokens will automatically be shipped to the provider's address on file. The user will receive an email from OMH Security containing a link to the Self-Service Console as well as a User ID and password to login to the Console. The email will also contain the hard token Enablement Code and token Serial Number that will be needed for the user to activate their hard token from within the Console, after they have received their hard token.

A policy for ensuring the protection of PHI should be shared with staff (e.g., staff must have HIPAA training before getting access to PSYCKES and login tokens should not be shared among staff; the organization's existing policies may be sufficient but should be reviewed, and possibly modified, in relation to PSYCKES.

Step 5: Security Manager revokes PSYCKES access for staff no longer requiring access

If the individual no longer requires PSYCKES access or has left the organization, the Security Manager disables the user's account in SMS. If the user had a hard (physical) token, the token should be mailed back to OMH. If the user had a soft (mobile-based) token, it is recommended that the token be removed from the individual's phone.