**Password Policy**

**Purpose:**

To establish a standard for creation of strong passwords, the protection of those passwords, and the frequency for changing those passwords. This policy only applies to passwords for accounts that access ePHI.

**Policy:**

1. Password construction
   1. One time use passwords will be created by the Information Security Officer and shared with the corresponding user via email or other messaging tool like Slack. The user will be required to log-in and reset their password within one hour.
   2. Access to the AWS account requires MFA with an approved device.
   3. Users must not use the same password across any two accounts.
   4. Users must not use the same password for Trialomics, Inc accounts as personal accounts.
   5. Each user’s password should meet the minimum requirements as outlined below :
      1. Must be a minimum of eight characters in length.
      2. Must contain a unique character.
      3. Must contain a number.
      4. May not contain your username or any part of your full name
      5. Passwords must not include easily guessed information such as personal information, names, pets, birth dates, etc.
2. Password change
   1. Passwords are not required to be changed. For critical systems that offer access to PHI, Trialomics, Inc enforces the use of MFA to access ePHI data.
3. Compromised passwords
   1. If a password is compromised, the Information Security Officer must be notified by the corresponding user and the password will be changed immediately.
4. Password protection
   1. Passwords must not be shared with anyone.
   2. Do not write down passwords and do not post them anywhere.
   3. Do not store passwords in documents that are not encrypted.
   4. Do not use the “remember password” feature on applications.
   5. Do not send passwords through email.
   6. Do not reveal passwords over the phone.
5. Password Storage
   1. Passwords for critical systems must be stored in a KeyPass file which grants access to at least one other individual.