**Mobile Devices Policy**

**Purpose:**

To allow for the authorized use of smartphones and other portable computing and communications devices at Trialomics, Inc by authorized members of the Trialomics, Inc Workforce.

**General Information:**

Mobile Devices can be used to provide better health care and more efficient administration. At the same time, the use of such devices creates new risks to patient privacy, Protected Health Information (PHI) and employee and organizational confidentiality, and intellectual property. This Policy is intended to permit the use of such devices while managing the risks they present.

**Definitions:**

1. Electronic Protected Health Information (ePHI): Individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.
2. User: Any employee or other person authorized by Trialomics, Inc to read, enter or update information created or transmitted via the electronic system.
3. Mobile Devices: Includes, but is not limited to smartphones, portable hard drives and USB (thumb) drives, digital music players, hand-held computers, laptop computers, tablet computers, and personal digital assistants (PDAs).

**Policy:**

1. In order to maintain the confidentiality and integrity of the Mobile Devices, Trialomics, Inc will:
   1. Never access, download, or store ePHI and metadata.
2. In order to ensure security for accessing systems that contain ePHI, Trialomics will use mobile devices for multi-factor authentication purposes.

**Procedures:**

1. This Policy applies to all electronic computing and communications devices which may be readily carried by an individual and is capable of storing, receiving, processing, or transmitting digital information, whether directly through download or upload, text entry, photograph or video, from any data source, whether through wireless, network or direct connection to a computer, other Portable Device, or any equipment capable of recording, storing or transmitting digital information (such as copiers or medical devices).
2. This Policy applies to personally-owned Mobile Devices as well as Mobile Devices owned or leased and provided by Trialomics, Inc.
3. In order to maintain the confidentiality and integrity of the Mobile Devices, Trialomics, Inc will:
   1. Never access, download, or store ePHI and metadata.
4. Authorization to Use Mobile Devices.
   1. No Mobile Device may be used for any purpose or activity involving information subject to this Policy without prior registration of the device and authorization by Trialomics, Inc. Authorization will be given only for use of Mobile Devices which Trialomics, Inc has been confirmed and configured to comply with this Policy..
   2. Access to, obtaining, use and disclosure of information subject to this Policy by a Mobile Device, and any use of a Mobile Device in any Trialomics, Inc facility or office, including an authorized home office or remote site, must be in compliance with all Trialomics, Inc policies at all times.
5. Authorization to use a Mobile Device may be suspended at any time:
   1. If the User fails or refuses to comply with this Policy.
   2. In order to avoid, prevent or mitigate the consequences of a violation of this Policy.
   3. In connection with the investigation of a possible or proven security breach, security incident, or violation of Trialomics, Inc policies
   4. In order to protect individual life, health, privacy, reputational and/or financial interests.
   5. To protect any assets, information, reputational or financial interests of Trialomics, Inc.
   6. Upon request of the department manager.
6. Authorization to use a Mobile Device terminates:
   1. Automatically upon the termination of a User’s status as a member of the Trialomics, Inc Workforce.
   2. Upon a change in the User’s role as a member of the Trialomics, Inc Workforce, unless continued authorization is requested by the department manager.
   3. If it is determined that the User violated this or any other Trialomics, Inc policy, in accordance with Trialomics, Inc policies.
   4. The use of a Mobile Device without authorization, while authorization is suspended, or after authorization has been terminated is a violation of this Policy.
7. Mobile Device User Responsibilities.
   1. In addition to other requirements and prohibitions of this and other Trialomics, Inc policies, Mobile Device Users have the following responsibilities:
      1. Information subject to this Policy, which is stored on the Mobile Device, must be encrypted as provided in Trialomics, Inc policy. Information subject to this Policy should not be stored on the Mobile Device for any period longer than necessary for the purpose for which it is stored.
      2. A Mobile Device may not be shared at any time when unencrypted information subject to this Policy is stored on the device.
      3. A Mobile Device which does not have unencrypted information subject to this Policy stored on it may be shared temporarily, provided that:
         1. The User may not share the password or PIN used to access the Mobile Device. The User may input the password or PIN for an alternate user in the event shared use is required.
         2. The configuration of the device, to comply with this Policy, must not be changed.
         3. The individual using the device, not the authorized user, must not further share it; must protect it against being misplaced, lost or stolen, and must immediately report to the User if it is; and must return it promptly to the authorized user when finished with the temporary use.
         4. The individual using the device must not use it to obtain, process, use or disclose information subject to this Policy.
      4. Access to each Mobile Device must be controlled by a password or PIN number consistent with Trialomics, Inc policy. Password or PINs must be changed periodically as provided in Trialomics, Inc policy. The Mobile Device must provide for a maximum of 3 attempts to enter the password or PIN correctly.
      5. The timeout for access to the Mobile Devices must be a maximum of 15 minutes.
      6. Information subject to this Policy which is transmitted wirelessly by the Mobile Device must be encrypted unless an exception is authorized. Exceptions must be authorized by the IT Department.
      7. If possible, Mobile Devices must have antivirus software. Mobile Devices that cannot support antivirus software may be subject to limitations on use at the discretion of the IT Department as specified in writing by the IT Department.
      8. Physical protection for Mobile Devices must be provided as required by Trialomics, Inc policy.
      9. Mobile devices shall not be left unattended in public areas.
      10. If the Mobile Device is misplaced, stolen or believed to be compromised this must be immediately reported to the Security Officer.
      11. Applications and services installed on the Mobile Device must be approved by the IT Department.
      12. Bluetooth and infrared (IR) services must be configured as approved by the IT Department or turned off.
      13. Mobile Devices must be disposed of according to Trialomics, Inc policy.
8. Personal Use of Mobile Devices.
   1. Personal Use of Mobile Devices owned or leased and provided by Trialomics, Inc is subject to the Trialomics, Inc Acceptable Use Policy.
   2. Personal use of personally owned Mobile Devices is not subject to the Acceptable Use Policy, but must at all times be consistent with this Policy.
   3. All information on a Mobile Device, including personal information about or entered by the User, may be subject to audit or evidentiary review as provided in this Policy. Any such personal information may be used or disclosed by Trialomics, Inc to the extent it deems reasonably necessary:
      1. In order to avoid, prevent or mitigate the consequences of a violation of this Policy.
      2. In connection with the investigation of a possible or proven security breach, security incident, or violation of Trialomics, Inc policies.
      3. In order to protect the life, health, privacy, reputational or financial interests of any individual.
      4. To protect any assets, information, reputational or financial interests of Trialomics, Inc.
      5. For purposes of determining sanctions against the User or any other member of the Trialomics, Inc Workforce.
      6. For purposes of litigation involving the User.
      7. If Required by Law.
9. Prohibited Uses of Mobile Devices.
   1. The following uses of Mobile Devices are prohibited:
      1. The storage of information subject to this Policy, including voice messages, photographs, voice notes, email, instant messages, web pages and electronic documents, images and videos, unless they are encrypted.
      2. The Internet, wireless transmission or upload of information subject to this Policy, including voice messages, photographs, voice notes, email, instant messages, web pages and electronic documents, images and videos, without encryption, unless previously authorized in writing by the IT Department.
      3. The creation of any photograph, image, video, voice or other recording of any individual who is a patient or member of the Workforce of Trialomics, Inc, except in compliance with Trialomics, Inc policy.
      4. The creation of any photograph, image, video, voice or other recording of any document, record, computer or device screen that includes information subject to this Policy, except in compliance with Trialomics, Inc policy.