Interoperability; Third-Party Application Registration Attestation

To use the Molina Healthcare, Inc. ("Molina") interoperability application programming interface ("API"), Molina requires third party application ("App") developers to attest to compliance with the standards listed below. If a developer fails to attest to compliance with these standards, Molina will notify any individual that requests his/her protected health information ("PHI") using the developer's App of that fact and recommend that the individual select an App from a different developer that has attested to complying with the following standards:

- The App has a comprehensive, easy-to-read, publicly available privacy policy, written in plain language, that has been affirmatively shared with the individual prior to the individual authorizing the App to access their PHI. To "affirmatively share" means that the individual must take an action to indicate they read the privacy policy, such as clicking or checking a box, and that the App developer has documented that the individual has taken such action.
- The App's privacy policy shall include, at a minimum, the following important information:
    - A description of how an individual's health information may be accessed, exchanged, or used by any person or other entity, including whether the individual's health information may be shared or sold at any time (including in the future);
    - An explanation to individuals regarding whether their PHI, after being provided to the App, will be subject to the privacy protections of the Health Insurance Portability and Accountability Act ("HIPAA") or other applicable privacy laws;
    - A requirement for express written consent from an individual before the individual's PHI is accessed, exchanged, or used, including receiving express written consent before an individual's PHI is shared or sold (other than disclosures required by law or necessary in connection with the sale of the App or a similar transaction);
    - Whether the App will access any other information from an individual's device; and
    - How the individual can discontinue use of the App and the App's access to their information, including what the App's policy and process is for securely disposing of an individual's information once the individual has discontinued use of the App.
- The App has reasonable and appropriate security safeguards in compliance with applicable laws and regulations, and consistent with the responsible stewardship associated with the protection of a user's personal information against risks such as loss or unauthorized access, use, alteration, unauthorized annotation, or disclosure.

For additional information about interoperability, please refer to CMS' website at www.cms.gov.