Developer Terms of Use

Application registration is available to you to submit FHIR API-based patient-facing applications ("Apps"), for use at healthcare organizations using iKnowMed. Apps submitted will be able to connect to the 2015 Edition CEHRT Release of iKnowMed and have chosen to enable APIs for this purpose. An App that uses any other APIs and/or have other users such as providers, will follow a different process and different terms may apply. You may use the iKnowMed FHIR API documentation as support in developing your App and submit it to McKesson as long as you follow these rules.

1. You agree to indemnify, hold harmless and defend iKnowMed, its subsidiaries, and their affiliates, and all of the employees, officers, directors, contractors and other personnel of any of them from and against any claim arising out of or relating to, directly or indirectly, you, any of your Apps, or any use of any of your Apps.
2. iKnowMed will issue a unique client identifier for each App you submit to keep track of which Apps use iKnowMed FHIR API. iKnowMed might need to suspend or revoke an App's client identifier if there are issues, concerns, or unsatisfactory reports regarding your App. If this happens, your App will not be able to communicate with iKnowMed systems until the concern is resolved and the suspended client identifier is restored.
3. Direct access to use iKnowMed software is not required to develop or test your App. Testing can be done via the iKnowMed FHIR API sandbox. Your registration and receipt does not give you permission to access iKnowMed software, and system. Your access to iKnowMed's software can ony be granted by McKesson.
4. You and Apps you submit must follow the FHIR App Development Guidelines, including documenting compliance to the ONC Certification Criteria.

Developer Guidelines

As an App developer, you are obligated to be familiar with principles for responsible healthcare App development and usage. As part of these responsibilities, you and Apps you submit must follow all of the below guidelines. If you or your Apps fail to follow these guidelines or misbehave in any other way, McKesson may take action on your Apps, including notifying users of your non-compliance, or suspending your App until the issue can be resolved. If you have reason to suspect your App is not following the guidelines or is misbehaving and would like McKesson to suspend use of your App until the issue is resolved, you can contact us at apiaccess@mckesson.com.

1. **Transparency.** Your pricing and marketing materials must be clear and consistent. You and your App must provide to users understandable financial and licensing terms that will apply to the use of your App. All information you provide about yourself, your organization, and your products must be accurate and truthful.
2. **Safety.** Your App must be designed and implemented to not put patients or your users at risk of harm. You may not use the Materials for any activities that could lead to death, personal injury, or damage to property. Your application must adhere to usability standards, specifically safety-enhanced design and accessibility-centered design.
3. **Security.** Your App must not pose a direct risk or otherwise increase the risk of a security breach in any system it connects to. Data exchange between your App and iKnowMed's APIs and between your App and any other third-party system must be secured with industry standard encryption while in transit, and use authentication and authorization protocols. Your App must secure all data on an end-user's device, and enforce inactivity time-outs. You and your App must not introduce any code of a destructive nature into any system you or your App conncect to. Your App's client identifier is given to you for your use only for a single App. You agree to keep your App's client identifier confidential, and will not disclose it to any third party, or use it for any other purpose.

4. **Privacy.** Your App must provide clear and understandable consent for use and give users the ability to decline consent. iKnowMed exclusively supports OAuth2.0 as the mechanism for authenticating acccess to patient data, and your App must not circumvent the display of any authentication or consent mechanisms from iKnowMed. You will provide and follow a privacy policy for your App that clearly, accurately, and truthfully describes to your users what data your App collects, and how you use and share this data. Your must not access, use, or disclose protected health information (PHI) or other confidential information in violation of any law or in any manner other than that which the owner of the information has given its informed consent.
5. **Sharing.** You may not share the data collected by your App with any third party without the explicit consent of the user of the App and the patient whose data is being shared.
6. **Reliability.** Your App must be properly tested and must be stable, predictable, and must not negatively impact clinical operations or patient safety for users. Development of your App must be documented and managed in a Quality Management System (QMS) and complaints and defects reported about your App must be managed in a complaint tracking system. If you identify a patient-safety, security, data breach, or privacy issue with one of your Apps, you must follow your documented compliant process to notify all users, and proactively contact iKnowMed to disable your App's usage until you resolve the issue.
7. **Efficiency.** Your App is not permitted to generate excessive load on a user's systems or to cause other systems to behave inaccurately or unexpectedly.
8. **Data Integrity.** You and your Apps must not corrupt or otherwise cause material inconsistencies in any data used by your Apps.
9. **Verifiability.** iKnowMed may inspect or test your App to verify your compliance with these guidelines and the FHIR API Terms of Use.

Developer Sign Up

1. Go to https://apiaccess.mckesson.com
2. Click Sign Up as a Developer
3. Enter the requested information. Please note the email address you enter will be your username for access to the iKnowMed API Portal.
4. Select I Agree with the iKnowMed API Portal's Terms of Service indicating your review and agreement.
5. Click Create Account. This will lead you to your Dashboard.

Required ONC Certification Criteria

To ensure minimum standards for safe and effective healthcare softward, you and your Apps must meet the below list of ONC certification criteria. For each App you submit, you must provide one of the following for McKesson and users to review:

- Public documentation that your App has been certified to the below specified ONC criteria.
- Public documentation of equivalent functionality in lieu of formal certification.
- Public documentation describing why specific criteria aren't applicable for your App.

McKesson may review documentation supplied by you at any time to ensure you meet these criteria. If documentation you supply is missing or inaccurate, McKesson may take action on your App, including notifying users of your App's non-compliance, or suspending your App until the issue can be resolved.

45 CFR 170.315 (b)(6)(Data Portability): "A user can configure the technology to create export summaries using the Continuity of Care Document document template."

45 CFR 170.315 (d)(1)(Access Control): "Verify against a unique identifier(s) (e.g., username or number) that a user seeking access to electronic health information is the one claimed; and […] establish the type of access to electronic health information a user is permitted based on the unique identifier(s) provided"

45 CFR 170.315 (d)(2) (Auditable Events): "The health IT record actions pertaining to electronic health information […] when health IT is in use; changes to user privileges when health IT is in use; and records the date and time [each action occurs]. […] The health IT records the audit log status […] when the audit log status is changed and records the date and time each action occurs. […] The health IT records the information […] when the encryption status of locally stored electronic health information on end-user devices is changed and records the date and time each action occurs.

45 CFR 170.315 (d)(3) (Audit Reports): "Enable a user to create an audit report for a specific time period and to sort entries in the audit log according to each of the data."

45 CFR 170.315 (d)(5) (Access Timeouts): "Automatically stop user access to health information after a predetermined period of inactivity. […] Require user authentication in order to resume or regain the access that was stopped."

45 CFR 170.315 (d)(7)(End-Device Encryption): "Technology that is designed to locally store electronic health information on end-user devices must encrypt the electronic health information stored on such devices after use of the technology on those devices stops [or] technology is designed to prevent electronic health information from being locally stored on end-user devices after the use of the technology on those devices stops."

45 CFR 170.315 (d)(8) (Data Integrity): "Verify […] upon receipt of electronically exchanged health information that such information has not been altered."

45 CFR 170.315(d)(9) (Trusted Connection): "Health IT needs to provide a level of trusted connection using either 1) encrypted and integrity message protection or 2) a trusted connection for transport."

45 CFR 170.315(g)(3) (Safety-Enhanced Design): "User-centered design process must be applied to each capability technology."

45 CFR 170.315(g)(4) (Quality Management System): "For each capability that a technology includes and for which that capability's certification is sought, the use of a Quality Management System (QMS) in the development, testing, implementation, and maintenance of that capability must be identified."

45 CFR 170.315(g)(5) (Accessbile Design): " The use of a health IT accessibility-centered design standard or law in the development, testing, implementation and maintenance of that capability must be identified."

45 CFR 170.315(g)(7) (Patient Selection): "The technology must be abel to receive a request with sufficient information to uniquely identify a patient and return an ID or other token that can be used by an application to subsequently execute requests for that patient's data."

45 CFR 170.315(g)(8) (API Access): "Respond to requests for patient data (based on an ID or other token) for each of the individual data categories specified in the Common Clinical Data Set and return the full set of data for that data category (according to the specified standards, where applicable) in a computable format."

45 CFR 170.315(g)(9) (CDA Access): "Respond to requests for patient data (based on an ID or other token) for all of the data categoreis specified in the Common Clinical Data Set at one time and return such data (according to the specified standards, where applicable) in summary record formatted [...] following the CCD document template."

45 CFR 170.523(k)(1) (Pricing Transparency): "Any additional types of costs that an EP, EH, or CAH would pay to implement the Complete EHR's or EHR Module's capabilities in order to attempt to meet meaningful use objecticves and measures."

45 CFR 170.523 (n) (Complaint Process): "Submit a list of complaints received to the National Coordinator on a quarterly basis each calendar year that includes the number of complaints received, the nature/substance of each complaint, and the type of complainant for each complaint."

Additional Proposed Suspension Criteria

In the future, ONC certification intends to also determine whether HIT modules are:

- *Contributing to a patient's health information being unsecured and unprotected in vioaltion of applicable law;*
- *increasing medical errors;*
- *decreasing the detection, prevention, and management of chronic diseases;*
- *worsening the identification and response to public health threats and emergencies; leading to inappropriate care;*
- *wosening health care outcomes;*
- *or undermining a more effective marketplace, greater competition, greater systems analysis, and increase consumer choice.*

You must acknowledge these goals as you develop your App.