Azalea Health's API 3rd Party Developer
Terms of Use
Last updated 10/26/2022

Terms of Use Documents

- API Documentation Terms of Use
- Developer Terms of Use
- Developer Guidelines
- Required ONC Certification Criteria
- Branding Guidelines
- MU3 API Vetting Guidelines

Overview

The following are core terms of use for interacting with and using the Azalea Health API. Please read and understand all below before registering for an Azalea Health Developer account, and before requesting an application to be vetted for access to the production Azalea Health system.

This information is available at the API Developer Portal (https://dev.azaleahealth.com). The developer portal is where you can register for an account, access the sandbox testing server, find documentation, and communicate with the Azalea Health API Team.

The API Documentation

We have made the documentation of Azalea's API (referred to as the "API Documentation") available to you for your development and testing. The API Documentation is provided to you as-is with no other warranties expressed or implied. You may use the API Documentation as long as you follow these rules:

1. The most recent Azalea API Documentation is located at https://devportal.azaleahealth.com.You can keep copies of the API Documentation for yourself, do not distribute them. Instead, link others to the API Documentation hosted on Azalea Health Developer portal website.
2. You own what you develop using the API Documentation. Azalea owns the API Documentation, as well as any improvements to or derivatives of the API

Documentation, such as enhancements to our testing tools or documentation. We want to encourage a vibrant developer environment, so if you suggest a way to improve the API Documentation and we use your suggestion, it may become part of the API Documentation for anyone to use without any obligation or notice to you.

3. You're responsible for your products and how they connect to the Azalea system, and the data within a user's account. You're also responsible for complying with all applicable laws, including not infringing on Azalea's or others' intellectual property rights.

Developer Terms of Use

Registration Process Requirements. Azalea Health's App Developer Portal registration is available to you to submit API-based Apps for use with healthcare organizations using Azalea Health (referred to as "Clients"). You may use documentation of Azalea's APIs (referred to as the "API Documentation") to develop Apps and submit them to devportal.azaleahealth.com as long as you follow these rules:

1. You agree to indemnify, hold harmless and defend Azalea, its subsidiaries, and Clients 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. You must create an Azalea User account and an Azalea Developer portal account to access and use the API. You must complete the registration process by providing current, complete, and accurate information when prompted. If any information changes, you agree you will promptly update your account information to reflect those changes.
3. Azalea will issue a unique client identifier for each App you submit to keep track of which Apps use Azalea's APIs. Azalea might need to suspend or revoke an App's client identifier if there is a concern with one of your Apps. If this happens, your App will not be able to communicate with the Azalea System until the concern is resolved and the suspended client identifier is restored. Contact Azalea Health to work on resolving the problem that led to the App's client identifier being suspended. Because it is possible that your App will be suspended, you will clearly inform users of your App that it might not always be available to them and that they should not rely on it in an emergency. You may not sell, transfer, sublicense, or otherwise disclose your account, unique client

identifier, or security credentials to any other party. You are responsible for maintaining the confidentiality of your account and credentials.

4. Direct access to Azalea Health's production system is not required to develop or test your products. Testing can be done via the Azalea Health API sandbox. Your receipt of the API Documentation does not give you permission to access the production Azalea Health system. Your access to the production Azalea Health system software can only be granted by Azalea Health.
5. You and Apps you submit on devportal.azaleahealth.com must follow the Azalea Health 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 those responsibilities, you and Apps you submit to devportal.azaleahealth.com must follow all of the below guidelines. If you or your Apps fail to follow these guidelines or misbehave in any other way, Azalea Health or Clients 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. If you have reason to suspect your App is not following the guidelines and would like Azalea Health to suspend use of your App until the issue is resolved, you can contact us at api@azaleahealth.com. Superscripts in the guidelines refer to ONC Criteria referenced in Required ONC Certification Criteria.

1. **Transparency.** Your pricing and marketing API Documentation must be clear and consistent. You and your App must provide to users and Clients understandable financial and licensing terms that will apply to the use of your Apps(k)(1). All information you provide about yourself 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(g)(3). You may not use the API Documentation 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(g)(3) and accessibility-centered design(g)(5)
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 Azalea Health's APIs and between your App and any other third-party system must be secured with industry standard encryption while in transit(d)(9),

and use authentication and authorization protocols(d)(1). Your App must secure all data on an end-user's device(d)(7) (d)(8), and enforce inactivity time-outs(d)(5). You and your App must not introduce any code of a destructive nature into any system you or your App connect 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. Azalea Health may provide a sanitized log of the activity of your App to Clients to review.

4. **Privacy.** Your App must provide clear and understandable consent for use and give users the ability to decline consent. Azalea Health exclusively supports OAuth 2.0 as the mechanism for authenticating access to patient data, and your App must not circumvent the display of any authentication or consent mechanisms from Azalea Health. 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 App 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, and without notifying the Client where the data originated. When sharing data, document what was shared, when, with whom, and for what purpose, and provide your users access to that documentation upon request(d)(3) (d)(11). Your App must provide the means for a user to export, transfer, or remove his or her data from application(b)(6).
6. **Reliability.**Your App must be properly tested and must be stable, predictable, and not negatively impact clinical operations or patient safety for users or Clients. Development of your App must be documented and managed in a Quality Management System (QMS)(g)(4) and complaints and defects reported about your App must be managed in a complaint tracking system(n). If you identify a patient-safety, security, data breach, or privacy issue with one of your Apps, you must follow your documented complaint process to notify all users(n), and proactively contact Azalea Health 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 Azalea Health'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(d)(2).

9. **Verifiability.** Azalea Health or Clients may inspect or test your App to verify your compliance with these guidelines.
10. **Reciprocity.** You will provide FHIR API-based Access[(g)(7) (g)(9)(g)(10)] to any data you and your App collect or derive to your users on the same terms as provided in these Development Guidelines.
11. **Fees.** There are no fees required to create a developer account or develop an application. If you choose to enter an agreement with Azalea Health to establish partner-level support and/or a comarketing agreement, any associated fees will be outlined in that agreement.
12. **Restrictions.** Subject to these Terms, Azalea grants you a limited, non-exclusive, revocable, non-transferable, and non-sublicensable right to access and use the Developer Portal, API and Azalea-owned content, documentation, code, and related materials made available to you on or through the Developer Portal or API (collectively, the “Materials”) in connection with the integration of your products and/or services with Azalea Health. Azalea may monitor your use of the API and Materials and use such information to improve the API and our services and to ensure your compliance with these Terms. All rights not expressly granted in the terms are reserved by Azalea and our licensors.

    You agree that in accessing or using the API or the Materials you will not:

    a. derive specifications from, reverse engineer, reverse compile, disassemble the API or Materials;
    b. use the API in a manner that materially delays, impairs, or interferes with system functionality of the API or Azalea Health for others or that compromises the security or integrity of any Azalea data, equipment, software, or system input or output;
    c. enter, transmit, or send data through the API, or deliver information to Azalea for publication to Azalea’s clients, that is illegal, threatening, harmful, lewd, offensive, defamatory, or that injures or infringes the rights of a third party;
    d. apply systems to extract or modify information from the API or Azalea using technology or methods such as those commonly referred to as "web scraping," "data scraping," or "screen scraping";
    e. use the API or Materials or any part or aspect of them for any unlawful purpose;
    f. sell, rent, lease, sublicense, redistribute, or syndicate access to the API, Azalea, or Materials to any third party without prior written approval from Azalea;

g. remove or alter any proprietary notices or marks on the API or Materials;
h. use or access the API for purposes of monitoring the availability, performance, or functionality of our services or for any other benchmarking purposes; or
i. cause, assist, or permit any third party (including an end-user) to do any of the foregoing.

13. **Limitations.** Your use of the API is subject to certain limitations on access, calls, and use as set forth in these Terms and input/output documentation and parameters available in the API reference materials in the Developer Portal. If Azalea believes that you have attempted to exceed or circumvent these limitations, we may temporarily or permanently block your ability to access and use the API and API Materials.
14. **Termination.** Azalea may change, suspend, or discontinue the API and suspend or terminate your use of the API and Materials, including any license granted hereunder, at any time for any reason, with or without notice. You may also terminate upon written notice to us by e-mailing api@azaleahealth.com.

Obligations. You agree to notify Azalea immediately at api@azaleahealth.com if you believe that your account or credentials have been compromised. Upon termination for any reason, you will: (i) not use the API or API Materials for any purpose whatsoever; (ii) immediately destroy or return to Azalea all material belonging to Azalea or our licensors, including without limitation all copies of the API, API Materials and our Confidential Information then in your possession or control; and (iii) certify to Azalea in writing that you have complied with the obligations listed above. The provision of this Section 15 shall not apply to the extent prohibited by Applicable Law (as defined below), including, without limitation, the 21st Century Cures Act.

Required ONC Certification Criteria

To ensure minimum standards for safe and effective healthcare software, 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 Azalea Health, Clients, 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

Azalea Health or Clients may review documentation supplied by you at any time to ensure you meet these criteria. If documentation you supply is missing or inaccurate, Azalea Health or Clients 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 Export):** "A user can configure the technology to create export summaries using the Continuity of Care Document document template."

45 CFR 170.315 (d)(1) **(Authentication, Access Control, Authorization):** "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 records 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 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 (d)(11) **(Accounting Disclosures):** "Record disclosures made for treatment, payment, and health care operations."

45 CFR 170.315 (g)(3) **(Safety-Enhanced Design):** "User-centered design processes 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) **(Accessible 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 able 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)(9) **(Application Access - All Data Request):** "Respond to requests for patient data (based on an ID or other token) for all of the data categories specified in the Common Clinical Data Set at one time and return such data (according to the specified standards, where applicable) in a summary record formatted [...] following the CCD document template."

45 CFR 170.315 (g)(10) **(Standardized API for Patient and Population services): "**Respond to requests for a single patient's data according to the standard adopted in § 170.215(a)(1) and implementation specification adopted in § 170.215(a)(2), including the mandatory capabilities described in "US Core Server CapabilityStatement," for each of the data included in the standard adopted in § 170.213. All data elements indicated as "mandatory" and "must support" by the standards and implementation specifications must be supported" and "Respond to requests for multiple patients' data as a group according to the standard adopted in § 170.215(a)(1) and implementation specifications adopted at § 170.215(a)(2) and (a)(4), for each of the data included in the standard adopted in § 170.213. All data elements indicated as "mandatory" and "must support" by the standards and implementation specifications must be supported.

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 objectives 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 violation 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;
- worsening health care outcomes;
- or undermining a more effective marketplace, greater competition, greater systems analysis, and increased consumer choice.

See Federal Register Vol. 81, No. 41, pg 11064 (3)

You will want to be mindful of these goals as you develop your App.

Branding Guidelines

Azalea Health's trademarks, service marks are available for use in promotional, advertising, instructional, or reference API Documentation, or on your websites, products, labels, or packaging once your application is vetted and running on the Azalea Health production system. The vetting process includes accepting guidelines for use of Azalea Health's brand. Examples of such guidelines:

- Your company is registered with Azalea Health.
- Azalea Health is not used as part of your product name.
- Your product has been successfully vetted by Azalea Health and is executing against the Azalea Health production system.
- Azalea Health is used in a referential phrase such as "live in production at", "compatible with" or "for use with."
- Azalea Health appears less prominently than your product's name.
- Azalea Health is not used in a way that could imply co-development, endorsement or sponsorship: You must always make a clear and unambiguous distinction between your own solutions, products, and/or services and the Azalea Health offerings.

MU3 Vetting Guidelines

Azalea Health is dedicated to allowing patients and providers to interact with health information from innovative 3rd party applications. Azalea Health also recognizes that it has a responsibility in protecting health information.

Any 3rd party application developer can connect to the Azalea Health Sandbox instance simply by signing up for a developer account at the Azalea Health Developer Portal (https://api-portal.azaleahealth.com). This gives full access to our Azalea Health API, as well as documentation on accessing and utilizing the MU3 API. This API covers the ONC required certifications (45 CFR 170.315 (g)(7), 45 CFR 170.315 (g)(8), and 45 CFR 170.315 (g)(9)).

Third party applications wishing to use the MU3 API to connect to our live azalea system will need to go through a vetting process. This process helps Azalea Health guarantee that the third party application correctly displays sensitive health information and is not a 'bad actor' (ex: an application whose only purpose is to steal health information).

Below is our vetting process and the criteria we use to vet MU3 API applications. MU3 API Vetting is a free service. We will never charge a fee for the MU3 API.

Vetting Process

- The third party developer will need to mark their application is ready for vetting on the Azalea API Developer portal. They will also need to provide the following information:
  - A description of the application and what is is designed to provide for Azalea Health Patients and/or providers.
  - Updated Contact information for Azalea Health to reach out to for vetting as well as future issues.
- A member of the Azalea Health API team will contact the developer within 21 work days to begin the vetting process. This process will require the developer to provide a way for the Azalea Health employee to test the application against the sandbox, or if that is impossible a walkthrough demo over a video conferencing link to ensure correct display of patient information and security. The developer will also need to supply and prove public posting of all the required documentation listed in Required ONC Certification Criteria.

We will NEVER deny an application for the following:

- Being a 3rd party competitor of Azalea Health.

We will deny an application for the following:

- Incorrect display of Healthcare information.
  - This includes inaccurate display of units on critical measures.
  - Information that does not belong to the patient being displayed
- An application that makes calls to the Azalea API that does not match either the oauth scopes registered for the application.
- An application that makes calls to the Azalea API that run counter to the description of the application provided.