BIDMC API DEVELOPER GUIDELINES

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 BIDMC API must follow all of the below guidelines based upon ONC Certification Criteria codified under 45 C.F.R. 170.315. If you or your Apps fail to follow these guidelines or misbehave in any other way, BIDMC 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 or is misbehaving and would like BIDMC to suspend use of your App until the issue is resolved, please contact BIDMC at ISProjectRequest@bidmc.harvard.edu. BIDMC may change and update these Developer Guidelines from time to time, and will publish any changes on this page. Make sure to check this page for any updates. Your continued use of the API after any such changes constitutes your acceptance of the new Developer Guidelines. **IF YOU ARE UNABLE TO COMPLY WITH ANY CURRENT VERSION OF THE TERMS, YOU SHOULD STOP USE OF THE BIDMC API IMMEDIATELY.**

Transparency. Your pricing and marketing materials must be clear and consistent. Clear and understandable financial and licensing terms that will apply to the use of your Apps must be made available to the public. All information you provide about yourself and your products must be accurate and truthful.

Safety. Your App must be designed and implemented to not put BIDMC's patients or your users at risk of harm. You may not use BIDMC API for any activities that could lead to death, personal injury, or damage to property.

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 BIDMC's API 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 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.

Privacy. Your App must provide clear and understandable consent for use and give users the ability to decline consent. The mechanism for authenticating access to patient data that is supported by BIDMC is OAuth 2.0, and your App must not circumvent the display of any authentication or consent mechanisms from BIDMC or individual BIDMC patients. You will provide and follow a privacy policy for your App that clearly, accurately, and truthfully describes to BIDMC patients and your users what data your App collects, and how you use and share this data, including uses anticipated for the future. Your App must not access, use, or disclose protected health information (PHI) or other confidential information in violation of any law, including state law under the Commonwealth of Massachusetts, or in any manner other than that which the owner of the information has given its informed consent.

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

Community Member 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.

Reliability. Your App must be properly tested and must be stable, predictable, and not negatively impact clinical operations or patient safety for patients, users or Community Members. 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. As soon as a patient-safety, security, data breach, or privacy issue with one of your Apps has been or should have been made known to you, you must follow your documented complaint process to notify all patients and users, and notify BIDMC within five (5) days to disable your App's usage at Community Member sites until you resolve the issue.

Data Integrity. All data received by you and your Apps must not modify the information received, including PHI, corrupt or otherwise cause material inconsistencies in any data used by your Apps.

Verifiability. BIDMC has the right to inspect or test your App to verify your compliance with these guidelines and the BIDMC API Terms of Use at any time without prior consent or authorization from you.

Reciprocity. You will provide BIDMC access to any data you and your App collect or derive to your users on the same terms as provided in these Development Guidelines.

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.

You will want to be mindful of these goals as you develop your App. *See* Federal Register Vol. 81, No. 41, pg 11064 (3).

5/22/19