



July 6, 2022

Subject: Tidepool public comments on *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions*, issued April 8, 2022

About Tidepool: Tidepool is an open source, 501(c)(3) non-profit organization that builds software for people living with diabetes. Tidepool develops:

- Tidepool Data Management Platform - a mobile and online platform that helps people with diabetes and their care teams.
- Tidepool Loop - an interoperable, automated insulin delivery (AID) system, currently under 510(k) review.

---

## Summary

Tidepool would like to be very clear on these key points:

- 1) Tidepool supports the rights of individual people living with diabetes to access their own personal health data, including real time glucose values and insulin delivery therapy data, from their diabetes devices, using whatever mechanisms they see fit, including but not limited to via secure digital device communication protocols and via secure cloud APIs. Tidepool also supports the right of these individuals to share their personal health data with anyone of their choosing, such as their healthcare provider / care team, researchers, as well as friends or family members.
- 2) Tidepool supports the rights of individual people living with diabetes to control their own personal diabetes devices using whatever methods they see fit.
- 3) Tidepool generally supports the intent of the guidance document, which is to encourage device manufacturers to develop secure devices, including devices that are Software as a Medical Device (SaMD), and to use a strong product development lifecycle and threat modeling to prevent unauthorized users from accessing data or controlling the devices.
  - a) **Tidepool strongly believes that all people living with diabetes are authorized users of their own devices. Tidepool encourages the Agency to make it clear in the guidance that individual patients / users of medical**

devices are considered *authorized users*, and that device manufacturers should enable secure, authorized access to such devices.

- b) Conversely, device manufacturers should NOT use cybersecurity mitigations as a mechanism to prevent patients / users (“authorized users” as described above) from accessing therapy data from their own devices, or from controlling their own devices.
- 4) Tidepool strongly believes that the individual rights expressed in points (1) and (2) do not in any way conflict with the goals of building a secure medical device. A secure medical device, hardware or SaMD, can simultaneously:
- mitigate cybersecurity threats using threat modeling, strong security controls providing confidentiality, integrity, and availability, as described in the guidance document
  - enable individuals living with diabetes to make their own choices about what software tools they use to access data and control their diabetes devices and therapy

While we support the Agency’s guidance and recommendations for device manufacturers to prevent unauthorized access or control of devices from malicious actors, we also strongly encourage the FDA to augment the guidance with a very clear statement that the guidance does not in any way preclude device makers from preventing individual patient users to make their own choices about:

- a) whatever software tools they use to access their personal health information from their devices
- b) what software tools they choose to allow control of their own devices

Tidepool believes that the risk of cybersecurity vulnerabilities is outweighed by the need for people living with diabetes to have control over managing their condition. But we also do not believe that the implementation of the recommended cybersecurity practices precludes this.

***Cybersecurity best practices should protect users, not restrict them. Following best practices for cybersecurity does not need to imply blocking patient users from accessing their own data or controlling their own devices. Tidepool asserts there is a risk that the FDA guidance will be interpreted or misinterpreted to suggest restriction of access by the patient user is appropriate or encouraged. The FDA can mitigate this risk by clearly stating a patient user’s access to and use of their own device can be considered authorized access, and should not be considered a cybersecurity threat.***

---

## Background and Rationale

As can be seen from the other public comments on this docket, a substantial contingent of the diabetes community feels very strongly that it is in their best interest to be able to use software and systems of their choice, and often feel that commercial systems fall short of providing the functionality that they desire to manage their condition.

The popularity of do-it-yourself systems such as Nightscout, OpenAPS, AndroidAPS and Loop demonstrates that many people are willing to use systems that have not been cleared or approved through traditional regulatory channels. The message from patients living with diabetes is clear: we want to be able to use tools of our choice to manage our condition, even if it means we have to develop these tools ourselves.

Fortunately, individual choice is not precluded by strong cybersecurity. Device makers can simultaneously:

- Follow a Secure Product Development Framework (SPDF) as described in the guidance, AND
- Allow individual users / patients to have secure access to data, and to control of their own devices

Two examples:

- 1) A hardware medical device manufacturer establishes a secure chain of trust based on a signed software and a certificate based authentication system. This design prevents unauthorized users (NOT the patient / user) from accessing personal health information from the device or controlling the device remotely.

The manufacturer also creates a mechanism that allows an individual user to establish credentials and download a certificate that enables them to access the data from their device, and to securely control their device using alternate software, based on published and validated device protocols.

- 2) A SaMD manufacturer creates a cloud-based system that stores real-time health information from one or more diabetes devices. The manufacturer creates cloud-based APIs that are secure and authenticated, but also allow for properly authenticated individual patients users to use those APIs to access their own data.

We note that secure mechanisms like this already exist in the consumer software and device space. These same mechanisms can be used securely in medical devices.

Tidepool also notes that our feedback on this matter is consistent with the FDA guidance offered in *“Manufacturers Sharing Patient- Specific Information from Medical Devices with Patients Upon Request”* issued October, 2017:

“Increasingly, patients seek to play an active role in their own healthcare. FDA is aware that sometimes a patient will request that a manufacturer share with her information about herself that has been recorded, stored, processed, retrieved, and/or derived from a legally marketed medical device...

Generally, if patient-specific information is shared with patients by manufacturers, it should be comprehensive and contemporary... the data should include all available data up through the most recent measurement. Manufacturers may also format the patient-specific information to facilitate its usability by the patient.”

Tidepool’s feedback is also consistent with this statement by former FDA Commissioner Scott Gottlieb, M.D.:

“We’re committed to continuing to identify new ways the agency can help foster transparency and patient access to accurate clinical information as a way to improve patient outcomes and health care delivery.”

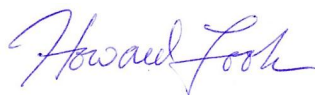
This statement was taken from the October 17, 2017 FDA brief, *“FDA in Brief: FDA encourages manufacturers to take steps to share personal health care data generated by medical devices with patients”* with the full text of the brief linked here;

<https://www.fda.gov/news-events/fda-brief/fda-brief-fda-encourages-manufacturers-take-steps-share-personal-health-care-data-generated-medical>

Tidepool believes that our feedback on the Cybersecurity draft guidance supports these goals, and supports patient-led innovation.

---

Tidepool genuinely appreciates the opportunity to provide these comments. Please let us know if you have any questions or would like to discuss our comments further.



Howard Look  
Founder and CEO, Tidepool  
<https://tidepool.org>  
[regulatory@tidepool.org](mailto:regulatory@tidepool.org)