Readout
Substance Workgroup Meetings
April 27 and 29, 2020

Thank you to everyone who joined and participated in our April meetings. Both meetings were conducted via teleconference due to the Coronavirus - COVID-19 and enjoyed productive and lively discussions. Over 25 people participated in the April meetings. A list of participants is included below.

As a reminder, the goal of this workgroup is to develop the content of a framework for unregulated health information. The April meetings focused on specific protections that should apply to covered data. Our upcoming meetings on May 18 and 20 will focus on exceptions to those protections. During the April meetings, the workgroup discussed on how baseline collection, use, and sharing limits of consumer health data should be addressed under the framework. There was also discussion regarding the definition developed during the March meetings.

Data rules under the framework:
During the April meetings, workgroup members discussed transparency and notice, consent, consumer controls, and corporate responsibilities sections. This summary will focus on the areas that garnered the most discussion during the April meetings. However, we also encourage workgroup members to provide additional feedback on each and every section of the April agenda. To aid in that endeavor, we have included the full list from the meeting's agenda in an appendix to this summary. One general consideration that was raised was for the workgroup to continue to address accessibility issues as the framework is developed, including accounting for the lack of accessible apps and products that collect or use health data.

1. Transparency and Notice
Transparency and notice serve two functions. First, they allow individual users to make an informed decision before they agree to participate to have their health information collected or used. Second, they allow researchers, regulators and advocates to track the big picture and trends on data use. The workgroup discussed ways for entities to provide users and enforcement authorities with information about how data will be collected, use, and shared.

The workgroup was encouraged to consider bifurcating the notice provisions. Specifically, one type of digestible and succinct notice would be provided to the consumer and another, more detailed and technical notice would be provided to an enforcement entity, researchers, and civil society groups. This approach provides users with the information they need without overwhelming them while simultaneously providing a parallel notice for regulatory and enforcement actions.

- ⇒ *Do workgroup members agree with this approach?*
    - *If yes - Would the framework require that the more complete notice reside on a public facing section of an entity's website?*

Participants also discussed the elements of consumer notice that identifies third parties with whom health data may be shared. Consumers should be provided more than simple generic use categories that fail to inform them about where their health data will end up. Our discussion centered around the level of detail that should be provided to users when their health data is shared. The workgroup considered if simply listing the categories of entities with whom the data will be shared is sufficient or if users should receive a list detailing specific entities. The group also discussed how feasible the latter approach is if entities do not know all the third parties that may ultimately receive shared data at the time notice is given to the consumer.

- ⇒ *Is there a middle ground where known third parties are disclosed to the user along with a specific list of additional types of third parties that may also receive the data at a later time?*

2. Consent

Consumer consent is one type of control governing the collection and use of health data. While this framework seeks to move beyond a basic notice and consent model with the addition of greater user controls and corporate obligations, there will still be instances when user consent is appropriate. Our discussion noted that there appears to be a greater desire to incorporate more granular controls and specify the scope of user consent, including the possible requirement for affirmative user consent before any health data can be collected. For example, some users may be more comfortable with collection and sharing when their health data is used for health purposes than for other commercial purposes, or only for use in certain services or pursuant to certain issues.

- ⇒ *Is the workgroup comfortable with this more granular and scoped approach to user consent?*

3. Consumer Controls

The workgroup devoted a significant amount of time to this section. Specifically, the discussion centered around users' abilities to correct and delete health information. While there was general consensus that there should be avenues that permit users to correct or delete their information, there were open questions about how entities should treat correction and deletion requests, and if certain types of health data sets should be subject to greater correction and deletion limits.

- ⇒ *Is the workgroup willing to add additional requirements along the following lines to this section of the framework?*
  - *An entity or person that collects or uses health information shall provide a user with a clear, easy process for requesting corrections to any inaccurate information?*
  - *Additionally, an entity or person that collects or uses health information shall make reasonable efforts to correct or delete an individual's health data based upon a user's request for correction or deletion?*

- *At minimum, an entity or person that collects or uses health information shall include a user's request to correct or delete health information within that user's health data?*
- *Should certain data always or never be available for correction or deletion?*
    - *For example - data that medical professionals may rely on.*

We also discussed how users' health data may be used by entities to train automated computer systems and AI.

⇒ *In an effort to stay consistent and offer users greater control of their health data under the framework, should we add a provision that provides users with the ability to opt into their data being used for the training of AI?*

4. Corporate Responsibilities

Currently, the burden of ensuring sufficient privacy protections around health data disproportionately falls on consumers. Workgroup participants discussed additional corporate responsibilities around data collection and use practices. Specifically, there was robust discussion around permissible secondary uses of health data.

⇒ *Other than what the data was originally collected or used for, are there any secondary uses of consumer health data that should be permitted under the framework?*

There was also discussion around incorporating greater responsibilities into the framework to include prohibitions on companies using health data to harm or discriminate against users through, for example, denials of housing, health services, employment, etc.

⇒ *Should the framework include a provision that prevents entities or persons that collect or use health information from using health information when making eligibility determinations around housing, health services, employment, and other critical determinations?*
    - *If yes - How do we ensure that we still permit the use of certain information, especially around access issues, to ensure equal access and accommodation considerations are permitted?*

Finally, we considered adding security provisions under this section. Specifically, these additional provisions would be designed to ensure that reasonable steps are taken to secure and protect consumer's health data.

⇒ *Should the framework include data security provisions, similar to those in existing frameworks and legislative proposals?*

The next sessions of this workgroup will focus on the specific protections and exceptions to the data covered by this working definition. Thank you all for your continued engagement and involvement with us on this project. We look forward to receiving your feedback. The next round of meetings for the substance workgroup will be later this month on May 18 and 20 via teleconference from 3:00 - 4:30 PM (EST).

Appendix

There are a range of protections that we can apply to consumer health data. For each section below, we have posed a series of questions for the workgroup to consider.

1. **Transparency and Notice**
    a. The goal here is to allow users to make an informed decision before they agree to participate to have their health information collected or used. An entity or person cannot collect or use health information unless it:
        i. *Clearly identifies the types of health information that will be collected?*
        ii. *Clearly states the purpose(s) that any health information is collected for?*
        iii. *States if any health information will be shared, and if yes, provide the user with the names of all the entities that will received, license, or purchase the shared health information?*
        iv. *States the reasons that any health information is shared?*
    b. Users should expect continued transparency and timely notice that reflect changes to how their health information is collected or used. An entity or person that collects or uses health information:
        i. *Must notify users when policies and practices surrounding how their health information will be collected or used have changed?*
    c. A privacy framework should encourage and facilitate accountability. An entity or person that collects or uses health information:
        i. *Must provide users with a description of the users' rights?*
        ii. *Must provide users a clear list of any user controls that are available?*

2. **Consent**
    a. Consent must be based on meaningful information that is separate from any set of terms and conditions. An entity or person cannot collect or use health information:
        i. *Until a user provides informed consent?*
    b. Consent should be granular and limited in scope. An entity or person collecting or using health information:
        i. *Must limit the collection of health information to only what the user has expressly consented to?*
        ii. *Must seek additional consent for any new collection or use of health information outside the scope of the original user consent?*
    c. User consent should be revocable. An entity or person collecting or using health information:
        i. *Must enable the ability for a user to subsequently revoke consent?*
        ii. *Must immediately stop the collection or use of health information once a user has revoked consent?*

3. **Consumer Controls**

a. User access to health information - An entity or person that collects or uses health information:
    i. *Shall permit individual users with the right to obtain a copy of their health information?*
    ii. *Provide consumers with the ability to access all identifiable health information about the user that an entity or person possesses?*
b. Users' ability to correct health information - An entity or person that collects or uses health information:
    i. *Shall provide a user with a clear, easy process for requesting corrections to any inaccurate information?*
    ii. *Shall provide users with information about who or what entity originally supplied the data, who made changes to the data, and what changes were made?*
c. Users' ability to delete health information - An entity or person that collects or uses health information:
    i. *Shall, upon a user's request, securely dispose of all of that user's health information?*
        - *with respect to any future uses or disclosures of user data?*
    ii. *Shall provide users a reasonable right to delete all of their health information?*
d. User portability rights – An entity or person that collects or uses health information:
    i. *Shall provide users with a general data portability right?*
e. Put a pin in discussions of limitations on individual consumer controls until our May meetings.

4. Corporate Responsibilities

a. Permissible collection and use practices – An entity or person that collects or uses health information:
    i. *Is not permitted to collect or use health information for any secondary use other than what the data was originally collected or used for?*
    ii. *Must limit the amount of health information collected or used to only what is necessary to carry out the operation a user has requested?*
    iii. *May only collect or use health information in a manner that is consistent with reasonable user expectations given the context in which the user provided or authorized the provision of the health information?*
    iv. *Shall minimize unnecessary data collection while still enabling functionality?*
    v. *Shall ensure that any third parties are prohibited from using or disclosing any user health information for any undisclosed purposes?*
b. Health information retention - An entity or person that collects of uses health information:

i. *Shall keep health information only as long as necessary to carry out the reason the data was collected or used, and after that, the data should be deleted?*
ii. *Shall delete all health data once there is no longer a valid reason to retain the data?*

April Substance Workgroup Meeting Participants

- David Brody
- Susan Bouregy
- Joanne Charles
- Corey Cutter
- Shari Erickson
- Dani Gillespie
- Carlos Gutierrez
- Michelle Huntley
- Deven McGraw
- Ben Moscovitch
- Hadly Clark
- Henry Claypool
- Robert Belfort
- Rachele Hendricks-Stirrup
- Laura Hoffman
- Varoon Mathur
- Dena Mendelsohn
- Mark Segal
- Alaap Shah
- Patricia MacTaggart
- Yael Weinman
- Alice E. Leiter
- Catherine Pugh
- Michelle Richardson
- Ridhi Shetty
- Andrew Crawford