DEPARTMENT OF HEALTH AND HUMAN SERVICES

Announcement of Requirements and Registration for "Privacy Policy Snapshot Challenge"

AGENCY: Office of the National Coordinator for Health Information Technology, HHS.

ACTION: Notice.

SUMMARY: The Model Privacy Notice (MPN) is a voluntary, openly available resource designed to help health technology developers who collect digital health data clearly convey information about their privacy and security policies to their users. Similar to a nutrition facts label, the MPN provides a snapshot of a product's existing privacy practices, encouraging transparency and helping consumers make informed choices when selecting products. The MPN does not mandate specific policies or substitute for more comprehensive or detailed privacy policies. The Privacy Policy Snapshot Challenge is a call for designers, developers, and health data privacy experts to create an online MPN generator. The statutory authority for this Challenge is Section 105 of the America COMPETES Reauthorization Act of 2010 (Public L. No 111-358).

DATES:

- Submission period begins: December 13, 2016
- Submission period ends: April 10, 2017
- Winners announced: May-June, 2017

FOR FURTHER INFORMATION CONTACT: Adam Wong, adam.wong@hhs.gov (preferred), 202-720-2866.

SUPPLEMENTARY INFORMATION:

Award Approving Official

B. Vindell Washington, National Coordinator for Health Information Technology.

Subject of Challenge

In 2011, the Office of the National Coordinator for Health Information Technology (ONC) collaborated with the Federal Trade Commission (FTC) and released a Model Privacy Notice (MPN) focused on personal health records (PHRs), which were the emerging technology at the time (view 2011 PHR MPN). The project's goals were to increase consumers' awareness of companies' PHR data practices and empower consumers by providing them with an easy way to compare the data practices of two or more PHR companies. In the last five years, the health information technology market has changed significantly and there is now a larger variety of products such as mobile applications and wearable devices that collect digital health data.

ONC recognized a need to update the MPN to make it applicable to a broad range of consumer health technologies beyond PHRs. More and more individuals are obtaining access to their electronic health information and using consumer health technology to manage this information. As retail products that collect digital health data directly from consumers are used, such as exercise trackers, it is increasingly important for consumers to be aware of companies' privacy and security policies and information sharing practices. Health technology developers can use the MPN to easily enter their information practices and produce a notice to allow consumers to quickly learn and understand privacy policies, compare company policies, and make informed decisions. Many consumer health technologies are offered by organizations that are not subject to the Health Insurance Portability and Accountability Act (HIPAA) privacy and security standards. This is detailed in the HHS report, Examining Oversight of the Privacy &

Security of Health Data Collected by Entities Not Regulated by HIPAA, released in July 2016 by ONC's Office of the Chief Privacy Officer with the cooperation of the HHS Office for Civil Rights (OCR) and the FTC.

The Privacy Policy Snapshot Challenge leverages updated content developed recently by ONC, with feedback from OCR, FTC, and other private and public stakeholders. The content also underwent informal consumer testing. The Privacy Policy Snapshot Challenge provides an award to the creators of the best MPN generator that produces a customizable MPN for health technology developers. The Challenge is a call for designers, developers, and health data privacy experts to create an online MPN generator that is easy for health technology developers to use in customizing a privacy notice that is compelling and understandable to consumers. Submissions will provide the code for an open source, web-based tool that allows health technology developers who collect digital health data to generate a customized privacy notice. The MPN generator must be able to produce privacy notices that adhere to the MPN content yet provide for customization by a health technology developer. Visit https://www.healthit.gov/sites/default/files/2016_model_privacy_notice.pdf to download the MPN.

The code for the web-based generator must be posted to GitHub and be available through an open source license such that any app developer can implement and use it. The solution should be developed as an HTML webpage styled using CSS (or SASS) that is powered by a framework, library, or plugin developed in JavaScript that is packaged and made available as one of the following:

- JQuery Plugin
- Node.JS Module

- Standalone Script

The final output of a successful submission is an MPN generator that can create customized privacy notices that would be accessible from an app or other consumer health technology; the privacy notices must, following the MPN, inform and educate the app or technology user so that they understand how the app or technology uses their personal health data. What the privacy notices created by the MPN generator look like and how they educate the user is up to the submitter – for example, the notices can be interactive or use graphics and images; however, it cannot be a simple static document such as a pdf. The MPN generator should create privacy notices that factor in accessibility, clean web design, and the differences between reading and understanding content on paper versus online, for which resources like Health Literacy Online (https://health.gov/healthliteracyonline/), the Draft U.S. Web Design Standards (https://standards.usa.gov/getting-started/), and Usability.gov can be helpful.

Submitters are also required to undertake consumer testing of the final customizable MPN produced by the MPN generator, which is intended to help bring in direct user feedback. Testing can be formal (such as standardized assessments or focus groups) or informal (such as among family members or individuals in a waiting room). Submitters must provide evidence of testing with at least five people. A larger amount of time spent with each tester, greater formal rigor, and the number and diversity of people used for testing will result in a more positive assessment under the selection criteria. Evidence demonstrating consumer testing could include sample feedback, quotes, or pictures, and should include how it affected development of the language, design, and/or structure of the customizable MPN. Resources like https://methods.18f.gov/discover/stakeholder-and-user-interviews/ can help.

Submission Requirements

Submitters must submit the following through the challenge webpage:

- Framework, library, or plugin file(s) for the MPN generator.
- ReadMe file that documents usage and installation instructions and system requirements (including supported browsers).
- Link to a demo webpage of the MPN generator.
- Slide deck of no more than ten slides that describes how the submission functions, addresses the application requirements, and includes evidence of consumer testing of the customizable MPN with a minimum of five people.
- Video demo (five minute maximum) showing implementation and use of the MPN generator and creation of the customizable MPN, and may also address consumer testing.
- Link to a Github Repository that includes the submission elements above. Submitters can make the Repository private so that their code is not out in the open during the submission and review phase, but are required to make it public if designated as challenge winners.

How to Enter

To enter this Challenge, submitters can access http://www.challenge.gov and search for "Privacy Policy Snapshot Challenge." On the challenge webpage, click "Submit Solution" and follow the instructions.

Eligibility Rules for Participating in the Challenge:

To be eligible to win a prize under this Challenge, an individual or entity:

1. Shall have registered to participate in the Challenge under the rules promulgated by ONC.

2. Shall have complied with all the stated requirements of the Privacy Policy Snapshot Challenge (parentheses above).
3. In the case of a private entity, shall be incorporated in and maintained a primary place of business in the United States, and in the case of an individual, whether participating singly or in a group, shall be a citizen or permanent resident of the United States.
4. Shall not be an HHS employee.
5. May not be a federal entity or federal employee acting within the scope of their employment. We recommend that all non-HHS federal employees consult with their agency Ethics Official to determine whether the federal ethics rules will limit or prohibit the acceptance of a COMPETES Act prize.
6. Federal grantees may not use federal funds to develop COMPETES Act challenge applications unless consistent with the purpose of their grant award.
7. Federal contractors may not use federal funds from a contract to develop COMPETES Act challenge applications or to fund efforts in support of a COMPETES Act challenge submission.
8. All individual members of a team must meet the eligibility requirements.

An individual or entity shall not be deemed ineligible because the individual or entity used federal facilities or consulted with federal employees during a Challenge if the facilities and employees are made available to all individuals and entities participating in the Challenge on an equitable basis.

Participants must agree to assume any and all risks and waive claims against the Federal Government and its related entities, except in the case of willful misconduct, for any injury, death, damage, or loss of property, revenue, or profits, whether direct, indirect, or consequential,

arising from my participation in this prize contest, whether the injury, death, damage, or loss arises through negligence or otherwise. Participants are required to obtain liability insurance or demonstrate financial responsibility in the amount of $500,000, for claims by a third party for death, bodily injury, or property damage, or loss resulting from an activity carried out in connection with participation in a Challenge.

Participants must also agree to indemnify the Federal Government against third party claims for damages arising from or related to Challenge activities.

General Submission Requirements

In order for a submission to be eligible to win this Challenge, it must meet the following requirements:

1. No HHS or ONC logo – The product must not use HHS' or ONC's logos or official seals and must not claim endorsement.
2. Functionality/Accuracy – A product may be disqualified if it fails to function as expressed in the description provided by the Submitter, or if it provides inaccurate or incomplete information.
3. Security – Submissions must be free of malware. Submitter agrees that ONC may conduct testing on the product to determine whether malware or other security threats may be present. ONC may disqualify the submission if, in ONC's judgment, it may damage government or others' equipment or operating environment.

Prize

- Total: $35,000 in prizes
- First Place: $20,000
- Second Place: $10,000
- Third Place: $5,000

Payment of the Prize

Prize will be paid by a contractor.

Basis upon Which Winner Will Be Selected

The review panel will make selections based upon the following criteria:

- Accurate use of MPN content, including appropriate modification of flexible language and no deviation from standardized language.
- Use and demonstration of best practices in developing and presenting web content for consumption, including consumer testing, web design, and accessibility, as exemplified in the resources provided above.
- Visual appeal of the generated MPN.
- Ease of use for a developer to implement and use the MPN generator, including ability to customize the MPN.

Additional Information

General Conditions: ONC reserves the right to cancel, suspend, and/or modify the Challenge, or any part of it, for any reason, at ONC's sole discretion.

Access: Submitters must keep the submission and its component elements public, open, and available for anyone (i.e., not on a private or limited access setting) on GitHub.

Open Source License: Winning submissions must use the open source MIT License.

Representation, Warranties and Indemnification

By entering the Challenge, each applicant represents, warrants and covenants as follows:

(a) Participant is the sole author, creator, and owner of the Submission;

(b) The Submission is not the subject of any actual or threatened litigation or claim;

(c) The Submission does not and will not violate or infringe upon the intellectual property rights, privacy rights, publicity rights, or other legal rights of any third party;

(d) The Submission does not and will not contain any harmful computer code (sometimes referred to as "malware," "viruses," or "worms"); and

(e) The Submission, and participants' use of the Submission, does not and will not violate any applicable laws or regulations, including, without limitation, HIPAA, applicable export control laws and regulations of the U.S. and other jurisdictions.

If the submission includes any third party works (such as third party content or open source code), participant must be able to provide, upon request, documentation of all appropriate licenses and releases for such third party works. If participant cannot provide documentation of all required licenses and releases, ONC reserves the right, at their sole discretion, to disqualify the applicable submission.

Participants must indemnify, defend, and hold harmless the Federal Government from and against all third party claims, actions, or proceedings of any kind and from any and all damages, liabilities, costs, and expenses relating to or arising from participant's submission or any breach or alleged breach of any of the representations, warranties, and covenants of participant hereunder.

ONC reserves the right to disqualify any submission that, in their discretion, deems to violate these Official Rules, Terms & Conditions.

Authority: 15 U.S.C. 3719

Dated: December 7, 2016

_____

Jon White,

Deputy National Coordinator for Health Information Technology.

BILLING CODE: 4150-45-P

[FR Doc. 2016-29718 Filed: 12/13/2016 8:45 am; Publication Date: 12/14/2016]