National Coordinator for Health Information Technology
U.S. Department of Health and Human Services 330 C Street SW
Washington, D.C. 20024

Re: Request for Information on Updates to ONC's Voluntary Personal Health Record Model Privacy Notice, 2016-04239

Dear Dr. DeSalvo:

As Vice-Chair of the Board of Directors of DirectTrust and Co-Chair of its Patient and Consumer Participation in Direct Work Group (PCP WG), I appreciate the opportunity to respond to this Request for Comment (RFC). Some DirectTrust colleagues are also pleased to contribute through this response.

The PCP WG of DirectTrust completed a Policy Opinion for the DirectTrust membership in February 2014 entitled "Fair Information Practice Principles for Privacy Policies of Non-HIPAA-Covered Entities v.1.0."[1] Discussion over several weeks by one-two dozen voluntary members of the PCP WG was guided by the concept of "privacy by design."[2] The result was a set of nine Principles, including text to explain the intent of each. The set is attached hereto as Exhibit 1. May I encourage you to consider them! The overall goal is disclosure to consumers and patients (consumers/patients) sufficient to reassure of protection of privacy and security in the event an individual decides to purchase/become subscriber of the offering from a non-HIPAA-covered entity. At the time, we were thinking of Personal Health Record (PHR) vendors.

Regarding the specific questions posed in the RFC:

1. User scope: Since the Model to be developed is voluntary, it would be ideal to direct it at all developers, not only non-HIPAA-covered. The more uniformity a consumer/patient encounters among these products, the better. The utter lack of such uniformity now is a serious barrier to understanding, acceptance, and appreciation of risks.
2. Information type: The notion that consumers/patients are going to parse different types of information does not seem realistic. Any information to be collected, including but not limited to identification factors, health records, physiological functions, must be disclosed.
3. Information practices: Please see Principles 4,5,6,7. Note we did not address de-identified data. I would add that any intent or practice to make such data available to third parties must be disclosed, including reasons therefore.
4. Sharing and storage: Consumers/patients have varying degrees of tolerance for their data being shared without their specific consent, *even for treatment, payment and operations*. If a non-HIPAA-covered entity intends to share PHI or PII with any party besides the consumer/patient, such sharing should be disclosed explicitly in language easily understood by consumers. Please see Principles 4 and 5.
5. Security and encryption: DirectTrust requires Level of Assurance (LoA) 3 for all entities tied to X.509 digital certificates in its Accredited Trust Anchor Bundle, *including consumers/patients*. DirectTrust believes that consumers/patients deserve no less security protection for and from relying parties. I urge ONC to address identity proofing in the Model Privacy Notice and if not urging this high level of identity assurance, explaining why not, including the risk of identity theft.[3] (Lots of sources for numbers of such thefts, sorry no time to furnish for you. PHI is much more valuable to such hackers.) Further, encryption both in transit and at rest should be required or at least recommended in the strongest terms. Recent data breaches in the health delivery and insurance sectors reveal serious lack of attention to security of consumer/patient PHI and PII. Information concerning the architecture and policies ensuring security should be available to consumers/patients in gradations of complexity: from "We protect your data..." to the specific technological specs that do this. Some consumers/patients won't want to know anything beyond an

[1] https://directtrust.box.com/s/gu36ub18vv4re61l3qhtcsfq4ik32a17 .
[2] GMSA. *Mobile Privacy Principles v.1.0*. London UK 2012. www.gsma.com/mobileprivacy.
[3] DirectTrust distinguishes identity proofing from authentication and operations management of security. The latter are not addressed here, although it can be noted that DirectTrust recommends two-factor authentication.

assurance. Others will want much more. The only reason not to disclose in full with clicks of a button is disinclination to be transparent or questioned.
6. Access to other device information: Frankly, this capability would dissuade me from any contact with such a product. Should be strongly discouraged.
7. Format: Any aggregation for transmission to third parties must be disclosed, the purpose explained, *and an option for opt-out be included*.
8. Information portability: no comment.

Note that Principles 1, 3, 8, and 9 are not addressed in the specific questions in the RFC. May I urge:

Principle 1: that ONC recognize that some consumers/patients will want to know more about the vendor than typically described on a web home page and prescribe elements of such notice, including those mentioned in Principle 1.

Principle 3: that ONC salute those consumer/patients who will want substantial control over their own PHI and PII and prescribe elements of Choice, Control, Consent and Correction that any Privacy Notice (and product!) should contain. Only a Model Notice is contemplated, not a law or rule. A Model may urge this be done, encourage developers to think about it.

Principle 8: that ONC acknowledge that non-HIPAA-covered entities are barely regulated (FTC oversight notwithstanding) and prescribe that such entities affirm their commitment to self-regulation consistent with Model Privacy Notice disclosures, including training within their organizations.

Principle 9: that ONC remind all entities targeted by the Model Privacy Notice that they are educating consumers/patients about private and secure health information exchange with every word they write or say and prescribe links to further sources of information about health information exchange, e.g. to ONC sites for consumers/patients.

To close, I highlight the importance of a simple, visual mechanism to assist consumers/patients to see a quick and concise description of privacy and security practices. The ability to get to the next level of detail regarding the practices should then just be a "click" away. For example:

- a standard checklist with a standard icon for each practice, a short description and a check whether the vendor engages in that practice;
- adopt the practice of web browsers to indicate a secure connection (e.g.: lock and the color green for the address space when an SSL certificate is valid.)

Thank you for chance to comment. If you have any questions, I will be happy to try to answer: ljohns@metacosmos.org or 415 361 4154. Looking forward to the draft Model.

Sincerely yours,

Lucy Johns, MPH
Vice Chair, Board of Directors, DirectTrust
Co-Chair, DirectTrust Patient and Consumer Participation in Direct Work Group

EXHIBIT 1

Principle 1. TRANSPARENCY (WHO)

The PHR system discloses prominent and timely information, in user-friendly language for consumers/patients, which identifies the entity and its privacy protection principles, policies and practices. Such information includes ownership, contact information that further describes the entity (mission, products, governance, etc.), and if it is non-profit, a link to its IRS 990 tax form. Note that the other Principles discussed below are only meaningful when a consumer/patient has notice of an entity's identity and the "privacy by design" framework that governs his or her rights within that framework.

Principle 2. PURPOSE AND USE (WHAT AND WHY)

The PHR system discloses prominent and timely information, in user-friendly language for consumers/patients, which defines the PHI and PII to be requested and collected, the authority that permits their collection, purposes for which the PHI and PII are intended to be used, particularly secondary uses, and to whom PHI and PII may be disclosed, under what circumstances, with and without consent.

Principle 3. CONSUMER/PATIENT CHOICE, CONTROL, CONSENT, CORRECTION (HOW)

The PHR system discloses opportunities, in user-friendly language for consumers/patients, to exercise meaningful choice and control over their PHI and PII. This entails many considerations, including but not limited to:

. any legal consumer/patient rights over the use of their personal information;

. consent concerning any use of PHI and PII by the PHR system;

. ability to delegate access to selected individuals and to revoke such access;

. designation of sources from which the PHR system may collect PHI;

. ability to view their PHI and PII in the PHR system's files, to ensure the accuracy and completeness of that information, and to tailor the information the consumer/patient may choose to reveal to others;

. information as to how any PHI and PII collected from consumers/patients may be used by the PHR system and ability for the consumer/patient to specify preferences regarding use;

. simple and easily-accessible ways for consumers to exercise their choices timely;

. full disclosure of charges if any.

Principle 4. DATA QUALITY AND INTEGRITY

The PHR system discloses, in user-friendly language for consumers/patients, how it ensures that PHI and PII are accepted and maintained to be accurate, relevant, timely, and complete (including revision history by the consumer/patient), including safeguards against corruption as the result of storage, retrieval or processing operations and citing both managerial (e.g. timely populating from designated sources) and technical (e.g. industry standard practices to ensure continuity of quality assurance across system and data boundaries) measures.

Principle 5. DATA SECURITY

The PHR system affirms, in user-friendly language for consumers/patients, awareness that PHI and PII can be sensitive information that the PHR system protects that information (in all media). The PHR system discloses its security safeguards against risks such as theft, loss, unauthorized access, revision or use, destruction, modification, and unintended or inappropriate disclosure. The PHR system also discloses its policy concerning Level of Assurance (LoA) used for consumer/patient identity management, including whether LoA used varies by use case within the PHR system. DirectTrust recommends LoA 3, similar to a consumer/patient HISP, for identity-proofing, authentication, credential management, and other operational policies pertaining to the PHR system.

Principle 6. DATA MINIMIZATION

The PHR system affirms, in user-friendly language for consumers/patients, that only the minimum PHI and PII relevant and necessary to accomplish the specified purpose(s) are collected and retained only for as long as necessary to fulfill the specified purpose(s) or to fulfill legal obligations.

Principle 7. LIMITATION ON USE

The PHR system affirms in user-friendly language for consumers/patients, that PHI and PII will be used solely for the purpose(s) specified, including any sharing of data with outside parties and for secondary purposes.

Principle 8. ACCOUNTABILITY FOR SELF-REGULATION

"It is generally agreed that...principles of privacy protection can only be effective if there is a mechanism in place to enforce them."[4] No such mechanism currently exists for PHR systems. The PHR system therefore affirms, in user-friendly language for consumers/patients, that it commits to self-regulation, including compliance with DirectTrust's Fair Information Practice Principles and training in their use and meaning for employees and contractors.

Principle 9. EDUCATION

Education of consumers/patients concerning privacy of their PHI and PII not being the responsibility of any authority within the HIE space, the PHR system affirms that it plays a role in such education, including disclosure of its privacy policy in conformance with these Principles and provision of links and contact information to additional resources for the interested consumer/patient.

[4] Federal Trade Commission. *Fair Information Practice Principles*. Washington DC 2012. www.ftc.gov/reports/privacy3/fairinfo.shtm