Journal of the American Medical Informatics Association, 28(3), 2021, 640–645
doi: 10.1093/jamia/ocaa227
Advance Access Publication Date: 11 December 2020
Perspective

Perspective

A proposal for shoring up Federal Trade Commission protections for electronic health record–connected consumer apps under 21st Century Cures

Raheel Sayeed,[1,2] James Jones,[1,] Daniel Gottlieb,[1,2,3] Joshua C. Mandel,[1,3] and Kenneth D. Mandl[1,2,3,*]

[1]Computational Health Informatics Program, Boston Children's Hospital, Department of Pediatrics, Harvard Medical School, Boston, Massachusetts, USA, [2]Department of Pediatrics, Harvard Medical School, Boston, Massachusetts, USA, and [3]Department of Biomedical Informatics, Harvard Medical School, Boston, Massachusetts, USA

***Corresponding Author:** Kenneth D. Mandl, MD, MPH, Computational Health Informatics Program, Boston Children's Hospital. 300 Longwood Avenue, Boston, MA 02115, USA; kenneth_mandl@harvard.edu

Received 19 August 2020; Revised 28 August 2020; Editorial Decision 31 August 2020; Accepted 9 September 2020

ABSTRACT

Under the 21st Century Cures Act and the Office of the National Coordinator for Health Information Technology (ONC) rule implementing its interoperability provisions, a patient's rights to easily request and obtain digital access to portions of their medical records are now supported by both technology and policy. Data, once directed by a patient to leave a Health Insurance Portability and Accountability Act–covered health entity and enter a consumer app, will usually fall under Federal Trade Commission oversight. Because the statutory authority of the ONC does not extend to health data protection, there is not yet regulation to specifically address privacy protections for consumer apps. A technologically feasible workflow that could be widely adopted and permissible under ONC's rule, involves using the SMART on FHIR OAuth authorization routine to present standardized information about app behavior. This approach would not bias the patient in a way that triggers penalties under information blocking provisions of the rule.

Key words: *patient data privacy, applications, medical informatics, health information system*

INTRODUCTION

For decades, a patient has been able to, under the Health Insurance Portability and Accountability Act (HIPAA), request a copy of their medical records in a "form and format" of their choice "if it is readily producible." However, the process is often onerous, inefficient, at times expensive, and almost always on paper.[1] There is recent progress. The 21st Century Cures Act[2] requires that certified health information technology provide access to all data elements of a patient's record, via application programming interfaces (APIs), that enable healthcare information "to be accessed, exchanged, and used without special effort." The Office of the National Coordinator of Health Information Technology (ONC) published a rule standardizing how patients can connect apps of their choice to their provider's electronic health record (EHR). With these substitutable[3]—easily added or deleted—apps, patients will be able to obtain a copy of a subset of their data (as defined by the U.S. Core Data for Interoperability), share it with healthcare providers and computerized processes that help them make decisions and navigate their care journeys, or contribute data to research. The rule specifies use of the SMART on FHIR (Fast Healthcare Interoperability Resources) API,[4] an open specification for launching apps[5] which is now part of the HL7 (Health Level Seven) FHIR standard.[6] As a result, these apps will soon run anywhere in the health system.

EMERGING APP MARKETPLACE

Apple advanced the app-based information economy[7] by connecting its native iOS "Health app" via the SMART on FHIR API to hundreds of health systems,[8] so that patients can download copies of their data to their iPhones. The 2020 ONC rule will no doubt spark development of many more apps.

Policymakers are grappling with concerns that data crossing the API and leaving a HIPAA-covered entity[9] are no longer necessarily governed by HIPAA (Figure 1). With the exceptions of apps hosted by a HIPAA-covered entity, or a not-for-profit entity, commercial apps and the data therein are regulated by the Federal Trade Commission (FTC) under Section 5(a) of the FTC Act (FTCA), which prohibits "unfair or deceptive acts or practices in or affecting commerce."[10] In this common scenario, a patient obtains their health data via an app after agreeing to the terms of service, or at least clicking through an agreement,[11] no matter how lengthy or opaque the language. The patient should always have access to the privacy policy. For commercial apps in particular, these policies are often poorly protective.[12] As with consumer behavior in the non-healthcare apps and services marketplace, we expect that many patients will broadly share their data with apps, unwittingly giving up control over the uses of those data by third parties.[13] Some patients may wish to explore the nascent marketplace offering options to monetize their data. "Information altruists"[14] and self-assembling patient groups will donate data[15] for innovation and research. The FTC does not regulate the content of terms or privacy policies. Because ONC's regulatory authority over EHRs does not extend to regulating consumer health apps, the new rule that promotes interoperability highlights a need for concomitant consumer protections.

How do we support patient autonomy to use tools of their choice while also protecting against predatory practices? While HIPAA does allow app developers to become business associates[9] of covered entities (e.g., a provider or healthcare institution) this arrangement only applies when an app is managing health information on behalf of the covered entity; in a consumer-centric ecosystem, many apps will instead have a relationship with a consumer directly. The covered entity itself may be a conflicted party when the patient wishes to use an app that either (1) shares data with a competing healthcare provider or (2) competes with the functionality of the entity's EHR. These conflicts could limit data flow across institutions, raising the barrier to entry for innovative apps. Further, the HIPAA business associate framework does not prevent un-consented commercial use of patient data. Data are already being widely shared in de-identified format on hundreds of millions of patients, without patient notification, and oftentimes aggregated, sold, and used for profit in ways that may enable downstream re-identification.[16]

A federal task force recognized that enabling patient autonomy to share data comes with inherent risk, and largely left these trade-offs in the patient's hands.[17] Solutions must include a mix of legislation, regulation, and best practices. We focus on strengthening the FTC's capacity to protect patients.

STANDARDIZABLE PRIVACY POLICY FOR HEALTH APPS

A first approach is to standardize the terms of service and privacy policies presented to consumers when interacting with EHR-connected apps. The ONC rule[18] requires that privacy notices for apps accessing a patient's electronic health information be provided in a nondiscriminatory manner, and be factually accurate, unbiased, objective, and not unfair or deceptive. They must further meet the requirements in Table 1.

We examined privacy risks highlighted by the ONC's 2018 Model Privacy Notice.[19] Elements in sample questionnaires that EHR vendors such as Epic (Epic Systems, Verona, WI) and Cerner (Cerner Corporation, Kansas City, MO) are already leveraging during security and privacy reviews of third-party applications, and

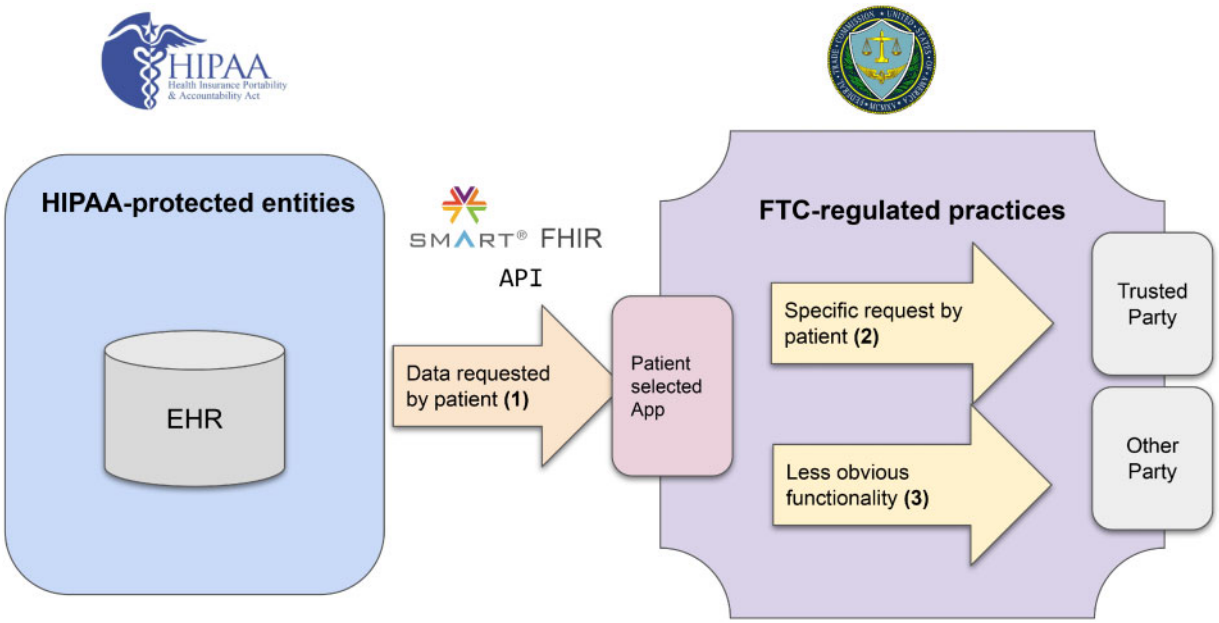

Figure 1. Regulatory landscape. Data flow from Health Insurance Portability and Accountability Act (HIPAA)–protected electronic health record (EHR) into an ecosystem of consumer-facing apps regulated by the Federal Trade Commission (FTC) and enabled by the SMART on FHIR (Fast Healthcare Interoperability Resources) application programming interface (API).

Table 1. Requirements for privacy policies introduced in the Office of the National Coordinator for Health Information Technology rule[18]

Requirement	Implication for privacy policies
Public and current	Policy must be made publicly accessible at all times, including updated versions.
Preemptively shared	Policy must be shared with all individuals that use the technology prior to the technology's receipt of EHI *from an actor.
Plainly informative	Policy must be written in plain language and in a manner calculated to inform the individual who uses the technology.
Data access transparency	Policy must include a statement of whether and how the individual's EHI may be accessed, exchanged, or used by any other person or other entity, including whether the individual's EHI may be sold at any time (including in the future).
Express consent	Policy must include a requirement for express consent from the individual before the individual's EHI is accessed, exchanged, or used, including receiving the individual's express consent before the individual's EHI is sold (other than disclosures required by law or disclosures necessary in connection with the sale of the application or a similar transaction).

EHI: electronic health information.

items addressed in the CARIN Alliance's code of conduct.[20] Leveraging an ecosystem of codes of conduct may be a complementary approach to any text in a privacy notice to a patient.

OPPORTUNITY USING SMART APP LAUNCH FRAMEWORK

The ONC rule standardizes the SMART on FHIR app launch framework[5] as a universal protocol for connecting third-party applications with EHRs. ONC's "information blocking" provisions in the rule require that apps be treated equally by provider organizations and EHR vendors. Hence, it could be construed as information blocking if an API developer (generally an EHR), or an API data provider (generally a healthcare organization) were to discourage a patient from connecting a particular app. There is an exception to information blocking on the basis of preventing harm, and the rule allows a healthcare provider to warn that an application has not attested to having adequate privacy policies. There is an opportunity, enabled in a technical workflow, for a non-discriminatory presentation of privacy policies of third-party patient-facing apps that may not be subjected to HIPAA; the "Certified API developer" (eg, EHRs) may seek attestation from the "API User" (app developer) as a "business associate and on behalf of a HIPAA covered entity" regarding their app's privacy practices. SMART includes a health-specific profile of the widely adopted open OAuth standard that allows apps to gain authorized access without the user having to disclose their credentials to the third-party app developer. As the app initiates the OAuth authorization routine ("App Authorization"), the user is explicitly redirected to an EHR's patient portal authorization interface, seeking approval for the app to access their data. This interface clearly identifies the app making the request along with the data elements (scopes) that the app is seeking from the EHR. Notably, Epic already administers a developer questionnaire addressing data privacy concerns when registering apps. What remains to be worked out is standardization and meaningful representation of these policies to the users during this approval dialog.

HEALTH "PRIVACY MANIFEST"

Within the SMART on FHIR specification, there is opportunity (1) to create a standardized privacy manifest with a minimal set of variables and text that distills an app developer's privacy policy for all actors (including the EHR vendors, health systems, and end users); (2) for app developers to declare this privacy manifest and have it shared within the EHR at the time of the app registration; (3) to relay and present the manifest in a non-discriminatory manner to the patient for access approval; and (4) for EHRs to monitor privacy policy changes by the app developer and trigger re-registration/re-attestation by the patient.

Privacy manifest categories

We summarize observed overlaps in approaches to address common data privacy concerns that consumers face when moving health data from a covered entity to a consumer app. Table 2 shows identified, standardizable data artifacts that can be reported by the app developer and communicated during the SMART workflow with minimal extra effort. Items rendered to the patient should be broadly understandable across literacy levels, diverse backgrounds, and languages. Badges representing certifiable trust entities that an app complies with can be leveraged here as well.

App registration with the EHR

In an OAuth framework, apps require a client identifier from the EHR along with its endpoints for data access. This is obtained during registration of the app. EHRs may capture the privacy manifest as part of this existing registration process by presenting a survey and capturing granular responses to specific privacy questions along with the regular elements that are part of the SMART specification. App developers may share a publicly accessible URI (uniform resource identifier) with the EHR pointing to the machine-readable privacy manifest artifact that can be rendered dynamically in the OAuth workflow.

Presenting the manifest to the user

Communicating the app's privacy manifest to the end user is possible at 2 stages prior to the app's use (Figure 2). First, app stores can display elements of the manifest as part of the app's listing, and even enable filters keyed off of these properties. Second, at application run time, as part of App Authorization within the SMART specification,[5] the EHR can evaluate the request and present an app authorization interface in the form of a web page to the user seeking their approval for allowing app access to the data (Figure 3). It is at this juncture that the privacy manifest would be populated into the authorization web page with the appropriate indications informing the user of the privacy policies pertaining to each of the categories of the manifest—"storage, usage, sharing, selling, consent for share"—and

Table 2. Proposed list of artifacts that can be captured from app developers and displayed to the patient during the SMART on FHIR authorization workflow

Artifact	Description
Privacy policy URL	Location of the full privacy policy for review.
Data storage policy	Information about how patient data is stored.
Data usage policy	Who can get access to full, de-identified, or aggregate patient data and what is the intent of its use?
Data sharing policy	Who may the app developer send the data to and for what purpose?
Data selling policy	What relevant data, if any, from the patient may be sold by the app developer?
Consent before sharing	The app's method for approaching patients before sharing their data with other parties.
Trust entities (badges)	Icons and links to any relevant trust entities claimed by the app developer.

FHIR: Fast Healthcare Interoperability Resources.

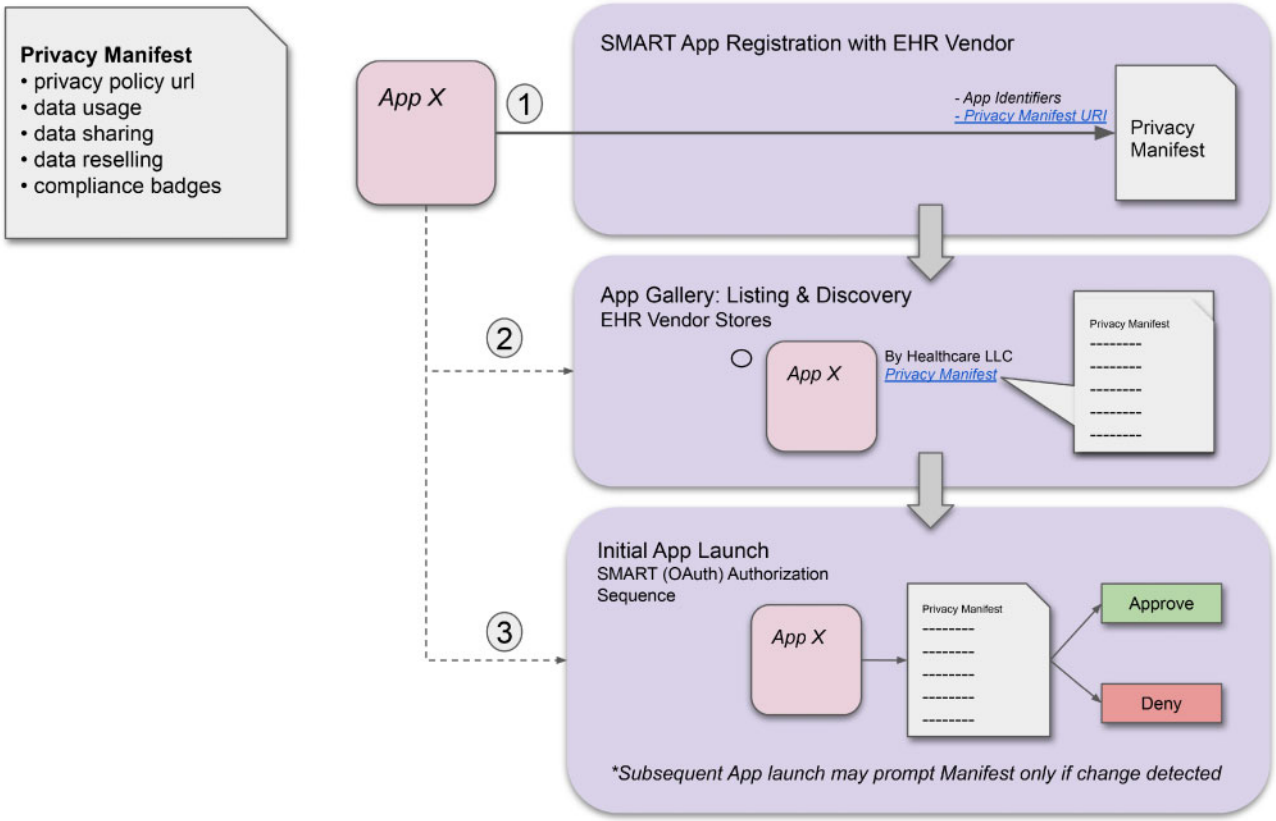

Figure 2. (1) App and its privacy manifest artifact are registered with the electronic health record (EHR). (2) EHR app galleries can present the manifest of registered apps prior to launch/installation. (3) At initial app launch by the user, or if prompted by a change in the app developer's policies, the EHR presents the manifest within the OAuth authorization sequence. Routine use of the app does not require presentation of the manifest unless a change is detected. URI: uniform resource identifier.

a URL link out to the privacy policy of the app. From here on, the user can either approve or deny the app's access to their data in the EHR.

Electronic provenance

The manifest itself should be a standardized, electronically transmissible document (e.g., in the form of a JSON resource), publicly hosted by app developers that is available to scrutiny at all times. App developers can be required to host and maintain a live, up-to-date manifest on their servers and declare the canonical URI to the EHR vendors during app registration. In turn, the EHR vendors, app stores, and research entities can detect changes to manifests through automated comparison with their local versions, and can take appropriate measures to require reauthorization or relay the change to the user during the app authorization routine (as described previously). Subsequent use of the app after the initial authorization flow should not otherwise require redisplay of the privacy manifest.

DISCUSSION

Our proposal guides app vendors toward attesting to app behavior in explicit, legally enforceable ways, and surfaces key details to consumers. The OAuth dialogue for communicating privacy policies

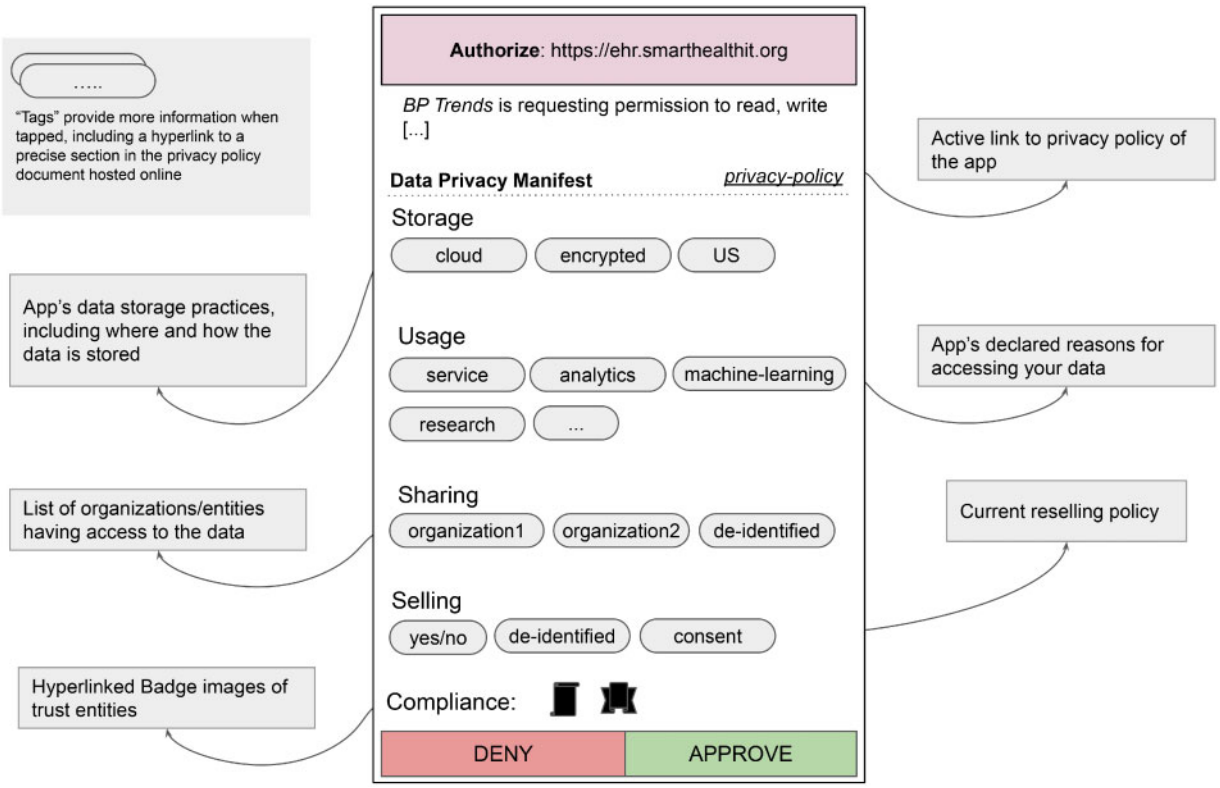

Figure 3. Prototype interface for electronic health record to present a summarized privacy manifest. Words and badges represented under "Storage," "Usage," "Sharing," "Selling," and "Compliance" can provide additional information when interacted with and can link out to the full-text privacy policy document from the app developer.

through a manifest is a viable step toward informing patients of potential implications of moving their health data into consumer apps. This approach should be augmented byon more robust privacy protections through regulation or comprehensive privacy legislation that defines elements of privacy policies and strengthens and funds FTC's role in enforcement. Developers can selectively declare compliance with recognized codes of conduct through certificates issued by the appropriate trust entities. This framework does not provide technical guarantees of app behavior; for example, a malicious actor may misrepresent practices. Further, not all app developers will fall under FTC oversight.

To protect patients from choosing a potentially malicious app without violating information blocking regulations, healthcare providers and payors could immediately begin presenting a privacy policy to the patient during the SMART on FHIR authorization routine, ensuring that the patient portals and authorization screens include links to an app's privacy policy. For EHR technology vendors, there is a further opportunity to test and potentially standardize a machine-readable privacy manifest with elements, tags, and artifacts that effectively relay the privacy behaviors of most apps. This manifest may include publishing a detailed privacy capturing artifact, provided by developers when registering the app, using existing FHIR resources (e.g., Questionnaire, QuestionnaireResponse).

FUNDING

This work was funded by 90AX0022/01-00 and 90AX0019/01-01 from the Office of the National Coordinator of Health Information Technology.

AUTHOR CONTRIBUTIONS

RS and KDM conceived and designed the privacy manifest. RS, JJ, KDM, JCM, and DG wrote the first draft. RS, JJ, KDM, JCM, and DG edited drafts. KDM provided funding.

CONFLICT OF INTEREST STATEMENT

RS and JJ have no competing interests. Boston Children's Hospital receives corporate philanthropic support for KDM's laboratory from SMART Advisory Committee members, which include the American Medical Association, the BMJ Group, Eli Lilly and Company, First Databank, Google Cloud, Hospital Corporation of America, Microsoft, Optum, Premier Inc, and Quest Diagnostics. KDM is an advisor to Medal and has advised Merck on use of real-world evidence. JCM is the chief architect for Microsoft Healthcare. DG is Principal, FHIR and Healthcare Data Standards for Central Square Solutions.

REFERENCES

1. Mandl KD, Kohane IS. Time for a patient-driven health information economy? *N Engl J Med* 2016; 374 (3): 205–8.
2. 114th Congress. H.R.34—21st Century Cures Act. Public Law 114-255. 2016.
3. Mandl KD, Kohane IS. No small change for the health information economy. *N Engl J Med* 2009; 360 (13): 1278–81.
4. SMART Health IT. Computational Health Informatics Program. https://smarthealthit.org Accessed August 18, 2020.
5. SMART App Launch Framework. http://www.hl7.org/fhir/smart-app-launch Accessed August 10, 2020.
6. HL7 FHIR Foundation. http://FHIR.org Accessed August 10, 2020.

7. Mandl KD, Mandel JC, Kohane IS. Driving innovation in health systems through an apps-based information economy. *Cell Syst* 2015; 1 (1): 8–13.
8. Mandl K. Apple will finally replace the fax machine in health care. *CNBC*. 2018. https://www.cnbc.com/2018/01/30/apple-will-finally-replace-the-fax-machine-in-health-care-commentary.html Accessed August 10, 2020.
9. Office for Civil Rights. Covered Entities and Business Associates. 2015. https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html Accessed August 10, 2020.
10. Federal Trade Commission Act. 2013. https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act Accessed August 13, 2020.
11. Cakebread C. You're not alone, no one reads terms of service agreements. *Business Insider*. 2017. https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11 Accessed August 10, 2020.
12. Sunyaev A, Dehling T, Taylor PL, *et al.* Availability and quality of mobile health app privacy policies. *J Am Med Inform Assoc* 2015; 22 (e1): e28–33.
13. Mandl KD, Kohane IS. Data citizenship under the 21st Century Cures Act. *N Engl J Med* 2020; 382 (19): 1781–3.
14. Kohane IS, Altman RB. Health-information altruists–a potentially critical resource. *N Engl J Med* 2005; 353 (19): 2074–7.
15. Taylor PL, Mandl KD. Leaping the data chasm: structuring donation of clinical data for healthcare innovation and modeling. *Harvard Health Policy Rev* 2015; 14 (2): 18–21.
16. Rocher L, Hendrickx JM, de Montjoye Y-A. Estimating the success of re-identifications in incomplete datasets using generative models. *Nat Commun* 2019; 10 (1): 3069.
17. Collaboration of the Health IT Policy and Standards Committees. API Task Force Recommendations. https://www.healthit.gov/sites/default/files/facas/HITJC_APITF_Recommendations.pdf Accessed August 10, 2020.
18. Health and Human Services Department. 21st Century Cures Act: interoperability, information blocking, and the ONC Health IT Certification Program. *Fed Regist* 2020; 85: 678.
19. Office of the National Coordinator of Health Information Technology. The Model Privacy Notice (MPN). https://www.healthit.gov/sites/default/files/2018modelprivacynotice.pdf Accessed August 10, 2020.
20. CARIN Alliance. CARIN Code of Conduct. https://www.carinalliance.com/wp-content/uploads/2019/05/2019_CARIN_Code_of_Conduct_05082019.pdf Accessed August 10, 2020.