A Technical Approach to Shore up FTC Consumer Protections for Electronic Health Record-Connected Apps

Raheel Sayeed, James Jones, Daniel Gottlieb, Joshua C. Mandel, Kenneth D. Mandl

Computational Health Informatics Program,

Boston Children’s Hospital, Boston, MA

A patient can, under the Health Insurance Portability and Accountability Act (HIPAA), request a copy of her medical records in a “form and format” of her choice “if it is readily producible.” However, patient advocates have long complained about a process which is onerous, inefficient, at times expensive, and almost always on paper. The patient-driven healthcare movement [1] advocates for turnkey electronic provisioning of medical record data to improve care and accelerate cures.

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 published digital connection points, known as application programming interfaces (APIs), that enable healthcare information “to be accessed, exchanged, and used without special effort.” In March, the Secretary of Health and Human Services announced a new rule, from The Office of the National Coordinator of Health Information Technology (ONC), facilitating a standard way for any patient to connect an app of her choice to her provider’s electronic health record (EHR). With these easily added or deleted (“substitutable” apps [3]), she should be able to obtain a copy of her data, share it with health care providers and apps that help her make decisions and navigate her care journeys, or contribute data to research. Because the rule mandates the ”SMART on FHIR” API [4] (an open standard for launching apps [5] that we developed, now part of Health Level Seven’s Fast Healthcare Interoperability Resources [6] ANSI Standard), these apps will run anywhere in the health system.

Apple recently advanced an apps-based information economy [7], by connecting its native “Health app” via the SMART on FHIR API, to hundreds of health systems [8], so patients can download copies of their data to their iPhones. The rule will no doubt spark the development of a substantial number of additional apps.

Policymakers are grappling with concerns that data crossing the API and leaving a HIPAA covered entity [9] are no longer governed by HIPAA. Instead, commercial apps and the data therein fall under oversight of 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].”

When a patient obtains her data via an app, she will likely have agreed to the terms of service or at least clicked through an agreement [11] no matter how lengthy or opaque the language. She should also have access to the privacy policy. For commercial apps in particular, these 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]. FTC does not regulate the content of terms or privacy policies.

Because ONC's regulatory authority over EHR does not extend to regulating consumer health apps, the new rule which promotes interoperability begs for concomitant protections for patients, who will naturally be drawn to use apps that help them manage their care and contribute to public health and research. Some patients may wish to explore the nascent emerging marketplace offering options to monetize their data. "Information altruists" [14] and self-assembling patient groups will donate data [15] to speed social and direct benefit through innovation and research. (Notably, the monetary value of an individual record is generally low, with exceptions for patients having rare or complex conditions and histories).

How do we support a patient's autonomy to use tools of her choice to improve her health and contribute to research, provide her with options to share in the monetary value from downstream uses of her data, while also protecting her from predatory practices?

HIPAA does not adequately address the issue. While it does allow an app developer to become a business associate [9] of a covered entity (such as a provider or healthcare institution) this arrangement only applies when an app is managing health information on behalf of the covered entity — whereas in a consumer-centric ecosystem, many apps will choose to have a relationship with a consumer directly. Importantly, 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 health care provider or (2) competes with the functionality of the entity's EHR. These conflicts could limit data flow across institutions, and raise the barrier to entry for new, innovative apps.

Further, the HIPAA business associate framework *does not* prevent commercial use of patient's data without consent. Patient data in de-identified format are already shared widely in healthcare on hundreds of millions of patients, generally in ways that are opaque and not reported to the patients whose data have oftentimes been aggregated, sold, and used for profit, and sometimes in ways that 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]. There are promising approaches available to protect a patient's health data without limiting choice or creating a bottleneck to innovation by new and smaller entrants into the Health IT ecosystem. Now is the time to consider these carefully.Ultimately, solutions will likely include a mix of legislation, regulation, and best practices. Here, we focus on strengthening the FTC's capacity to protect patients, exploring two pathways.

Methods

Our first approach is to standardize the terms of service and privacy policies presented to consumers when interacting with EHR-connected apps:

The extended federal responses to comments on the ONC rule [18] require that privacy notices for apps accessing a patient's electronic health information (EHI) must be at a minimum (1) made publicly accessible at all times, including updated versions; (2) shared with all individuals that use the technology prior to the technology's receipt of EHI from an actor; (3) written in plain language and in a manner calculated to inform the individual who uses the technology; (4) 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); and (5) 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).

In the interest of allowing information to flow freely, the commentary further suggests [19] that patient-facing privacy notices should be focused on any current privacy and/or security risks posed by the technology or the third-party developer of the technology. They are also encouraged to be provided in a non-discriminatory manner, factually accurate, unbiased, objective, and not unfair or deceptive.

To consider the realizability of these requirements, we analyzed privacy risks touched on by the ONC's 2018 Model Privacy Notice,[20] elements in sample questionnaires that EHR vendors are already leveraging during security and privacy reviews of third-party applications, and items addressed in codes of conduct such as the CARIN Code of Conduct [21]. We note here that leveraging an ecosystem of codes of conduct may be a complementary approach to any text in a privacy notice to a patient, as many current privacy practices are difficult to capture succinctly.

Table 1 summarizes observed overlaps in approaches to address common data privacy concerns consumers face when moving health data from a covered entity to a consumer app.

Data Privacy Concern:	**Listed in 2018 Model Privacy Notice**	**Observed in EHR app developer questionnaire**	**Addressed in CARIN Code of Conduct**
Is all or some of the data you collect covered under HIPAA?	Y	Y	Y
How is identifiable data used internally?	Y	Y	Y
How is identifiable data shared?	Y	Y	Y
How is de-identified data shared or sold?	Y	Y	Y
Where is de-identified data sold?	Y	Y	Y
Where is identifiable data stored?	Y	Y	Y
When is data encrypted?	Y		Y
Is the user allowed to (access/edit/share/delete) their data?	Y	Y	Y

What happens to your data when your account is deactivated?	Y	Y	Y
How are users notified in the case of an improper disclosure?	Y		Y
What potential impact does sharing this data have on others including your family?			Y
Is this a one time collection of data or authorization for future access?			Y
Are user changes to data able to be viewed when that data is shared with other parties?			Y
What happens to user data under transfer of ownership by the developer?			Y

Table 1. Approaches to identifying current privacy risks.

The SMART on FHIR specification [5] is standardized in the ONC rule as a universal connector between third-party applications and an EHR. SMART includes a health-specific implementation of the widely adopted open standard OAuth 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 authorization interface by the EHR to seek approval for allowing the app access to her data. This interface clearly identifies the app making the request along with the data (scopes) the app is seeking from the EHR. This technical underpinning of the app authorization process provides an opportunity for a dialogue with the patient.

Results

Within the SMART on FHIR specification, we have identified opportunities (1) to create a standardized *privacy manifest* with a minimal set of variables and text that attempts to distill 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 with the EHR at the time of the app registration and (3) for EHRs to relay and present the manifest in a non-discriminatory manner to the patients for access approval.

Privacy Manifest Categories. Communicating the Privacy Manifest is technically accomplishable as part of the SMART specification within its “App Authorization sequence (described above) that is also referenced in the ONC rules– in a response to the privacy policies of third party patient-facing apps that are not subject to HIPAA [18]. Box 1 shows identified data artifacts which can be reported by the app developer and communicated during the SMART workflow with minimal effort. Care must be taken to ensure the items rendered to the patient are accurate and broadly interpretable and understandable across literacy levels and diverse backgrounds, including different native languages.

Artifact able to be captured from app developers and then displayed to the patient during SMART on FHIR authorization	**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

App registration with the EHR. Apps require a client identifier from the EHR along with its endpoints for data access. This is obtained after registration of the app. EHRs may capture the privacy manifest as part of this existing registration process by presenting a survey and capturing granular "yes or no" responses to specific privacy questions along with the regular elements that are part of the SMART specification

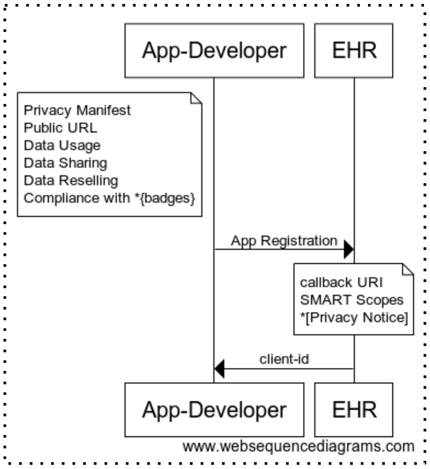

Figure 1. App registration with the EHR. The EHR performs a privacy and security evaluation with the app developer prior to registration and populates the app's SMART Scopes and privacy manifest then shares the client-id with the App

developer.

Presenting Manifest to the User. When the end-user launches the app, the app seeks authorization to access the EHR, at which point the EHR evaluates the request and presents an app authorization interface in the form of a web page to the user seeking her approval for allowing app access to the data. It is at this juncture, that the "privacy manifest" is populated into the authorization web page with the appropriate level of "caution" or "warning" indication informing the user of the privacy policies pertaining to each of the categories of the manifest– "*storage, usage, sharing, selling, consent for share*" and a url link out to the privacy policy of the app. From here on, the user has two choices: either approve the app's access to her data in the EHR or deny.

Discussion

Transparency in apps' sharing policies with regards to research use and monetization can empower patients to decide to share more data with good actors and avoid those apps unwilling to meaningfully disclose their practices. We view leveraging the OAuth dialogue for communicating privacy manifests as a potentially critical intermediate step to inform patients of the implications of moving their health data into consumer apps, pending more robust privacy protections or strengthening of FTC enforceability. These manifests can serve all modalities of a third-party app (web or device native) and can additionally be absorbed by smartphone app stores to be rendered to the user upon installation of the app.

Further consultation with stakeholder experts is needed to iterate upon a common, standardizable manifest with granular questions able to extract key elements of a patient health privacy policy. Of note, EHR vendors or providers are able to require updates to the manifest from app developers as needed, reaffirming privacy policies on emergent issues to patients.

References

1. Mandl KD, Kohane IS. Time for a Patient-Driven Health Information Economy? *N Engl J Med.* Jan 21 2016;374(3):205-208.

2. 114th Congress. H.R.34 - 21st Century Cures Act; 2015-2016.

3. Mandl KD, Kohane IS. No small change for the health information economy. *N Engl J Med.* Mar 26 2009;360(13):1278-1281.

4. Computational Health Informatics Program. SMART Health IT. http://smarthealthit.org.

5. HL7, Computational Health Informatics Program BCsH. SMART Application Launch Framework Implementation Guide Release 1.0.0. http://www.hl7.org/fhir/smart-app-launch/.

6. HL7. HL7 FHIR Foundation. http://www.fhir.org/.

7. Mandl KD, Mandel JC, Kohane IS. Driving Innovation in Health Systems through an Apps-Based Information Economy. *Cell Syst.* Jul 2015;1(1):8-13.

8. Mandl KD. Apple will finally replace the fax machine in health care. *CNBC https://www.cnbc.com/2018/01/30/apple-will-finally-replace-the-fax-machine-in-health-care-commentary.html*; 2018.

9. Services DoHaH. Covered Entities and Business Associates. *HHS.* [https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

10. *. Title 15 U. S. Code §45.*

11. Cakebread C. You're not alone, no one reads terms of service agreements. *Business Insider* [https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11?r=UK.

12. Sunyaev A, Dehling T, Taylor PL, Mandl KD. Availability and quality of mobile health app privacy policies. *J Am Med Inform Assoc.* Apr 2015;22(e1):e28-33.

13. Mandl KD, Kohane IS. Data Citizenship under the 21st Century Cures Act. *N Engl J Med.* Mar 11 2020.

14. Kohane IS, Altman RB. Health-information altruists--a potentially critical resource. *N Engl J Med.* Nov 10 2005;353(19):2074-2077.

15. Taylor PL, Mandl KD. Leaping the Data Chasm: Structuring Donation of Clinical Data for Healthcare Innovation and Modeling. *Harvard Health Policy Rev.* Spring 2015;14(2):18-21.

16. Rocher L, Hendrickx JM, de Montjoye YA. Estimating the success of re-identifications in incomplete datasets using generative models. *Nat Commun.* Jul 23 2019;10(1):3069.

17. Committee HIPaS. API Task Force Recommendations. https://www.healthit.gov/sites/default/files/facas/HITJC_APITF_Recommendations.pdf.

18. Office of the National Coordinator of Health Information Technology. 21st Century Cures Act: Interoperability Information Blocking and the ONC Health IT Certification Program. *45 CFR Parts 170 and 171 RIN 0955-AA01. Page 678*; 2020.

19. Office of the National Coordinator of Health Information Technology. 21st Century Cures Act: Interoperability Information Blocking and the ONC Health IT Certification Program. *45 CFR Parts 170 and 171 RIN 0955-AA01. Page 675*; 2020.

20. Office of the National Coordinator of Health Information Technology. The Model Privacy Notice (MPN) https://www.healthit.gov/sites/default/files/2018modelprivacynotice.pdf.

21. CARIN Alliance. CARIN Code of Conduct. https://www.carinalliance.com/wp-content/uploads/2019/05/2019_CARIN_Code_of_Conduct_05082019.pdf.