Comments of Anna Slomovic, PhD
Regarding 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program

Delivered via the Federal Rulemaking Portal at http://www.regulations.gov

U.S. Department of Health and Human Services
Office of the National Coordinator for Health Information Technology
Mary E. Switzer Building, Mail Stop: 7033A
330 C Street SW, Washington, DC 20201

Re: RIN 0955-AA01, dated March 4. 2019

I appreciate the opportunity to submit comments on the Office of the National Coordination for Health Information Technology (ONC) proposed rule to implement certain provisions of the 21st Century Cures Act. The proposal appears in the *Federal Register*, Vol. 84, No. 42, p. 7424.

I am a consultant and a scholar, affiliated with George Washington University's Cyber Security & Privacy Research Institute (CSPRI). For 15 years prior to returning to consulting and research, I held various corporate positions, including positions as Chief Privacy Officer (CPO) of companies ranging in size from start-up to Fortune 500. One of these organizations was a nation-wide behavioral health plan with 25 million members and a presence in almost every state and in every healthcare market (ERISA-regulated employer health plans, state-regulated insurers, Medicaid, and Tricare). I was responsible for the development and implementation of all privacy policies and procedures for data access and disclosures in that organization. I was also CPO of a consumer-facing online health education and services company, which provided a Personal Health Record (PHR) that allowed consumers to collect their medical data in one place. Additionally, I have served on federal and state-level work groups and commissions dealing with electronic health information exchange and PHRs, as well as on a national committee to create a US national identity verification standard. You can find additional information about my background on my website, www.annaslomovic.com. These comments reflect my own views and not the views of George Washington University, CSPRI, or any member of the university's faculty or staff.

I commend the Department of Health and Human Services for its efforts to ease access by individuals to their own medical information. Although the right of access was codified in the HIPAA Privacy Rule almost 20 years ago, patients' access to their own data often remains difficult and expensive. Many organizations provide patients with access to specific data elements like test results or claims, but this access is generally not intended to be a substitute to the right of access to the complete Designated Record Set as required under HIPAA. In addition to facilitating access, the proposed rule also facilitates export of data and makes it easier for patients to move data as they move through the continuum of care.

I also commend ONC for expanding the definition of information subject to access by the individual. Inclusion of information "directly from an individual, or from technology that the individual has elected to use" (p. 7513) makes it more likely that the individual will get all data related to him or her.

However, we must make sure that increased access to data does not harm those it is supposed to help. My comments on the NPRM fall into three categories: access to and disclosure of health data; identity and patient record matching; and the need to strengthen the patients' ability to correct or amend their records, which is missing from the rulemaking.

Access and disclosure

The proposed rule turns the HIPAA Privacy Rule on its head. As noted on p. 7527, HIPAA permits but does not require information disclosure in most circumstances. Patient access to their own data is one of the few cases in which the HIPAA Privacy Rule requires disclosure. In contrast, the ONC proposed rule requires disclosure in all circumstances unless an exception applies. By requiring disclosure the proposed rule risks undermining the protections of the HIPAA Privacy Rule. Exceptions and sub-exceptions in the proposed rule are not sufficient to allay this concern.

ONC notes that its privacy exception and sub-exceptions mirror the requirements of state and federal privacy laws. (p. 7526) In combination with the reversal of the HIPAA approach to data disclosure, the ONC rule will prevent providers from offering greater privacy protections to their patients than required by law. This approach does not recognize that the HIPAA Privacy Rule was intended as a "floor" of privacy protection, not a "ceiling." Many states either don't have privacy laws that cover health information or have relaxed their privacy protections to be "consistent" with HIPAA. Allowing multi-state organizations to implement policies that comply with the strictest laws in at least one state (p. 7528) is helpful, but it will penalize patients who use providers operating in a single state that does not have adequate protections for health information. I urge ONC to adopt the HIPAA Privacy Rule approach that permits but does not require disclosure except to the patient, the Secretary, and in other cases specified in the HIPAA Privacy Rule.

In addition to the general concern about the disclosure regime, I have some specific concerns and suggestions for addressing them.

Disclosure to the individual or individual's representative

I am alarmed by ONC's statement that "[d]isagreement with the individual about the worthiness of the third party as a recipient of EHI, or even concerns about what the third party might do with the EHI, except for reasons such as those listed in the "preventing harm" exception, are not acceptable reasons to deny an individual's request." (p. 7536) This statement reflects the position of the HHS Office for Civil Rights, as stated in its recent guidance on apps and patient right of access. However,

in combination with the ONC prohibition on vetting apps (p. 7486), the proposed rule opens the door to the acquisition and distribution of sensitive health information by unscrupulous app developers.

Dr. Donald Rucker, National Coordinator for Health IT, has stated that it should be up to patients "to decide whether the potential benefit of an app to manage their health care information and medical conditions outweighs potential risks."[1] Unfortunately, the notion that patients are in a position to make an informed tradeoff between the costs and benefits of using apps is a fallacy. As shown by multiple studies, individuals often have no way of knowing how apps use and disclose their information, or what they are agreeing to when they grant permissions to an app.[2] Research shows that many apps have poor security[3] and that users are significantly more vulnerable to attacks on mobile devices than on desktops.[4] The use of apps may not be a tradeoff between cost and benefit but an expression of resignation to the fact that it is impossible to live in a modern society without using apps and devices that violate one's privacy.[5]

The fact that patients will need to authenticate through the app can make matters worse since it can allow a malicious developer to steal and sell patient access credentials.

---

[1] Statement of Donald Rucker, M.D., National Coordinator for Health Information Technology Office of the National Coordinator for Health IT Department of Health and Human Services, before the Senate Committee on Health, Education, Labor and Pensions, May 7, 2019, https://www.help.senate.gov/imo/media/doc/Rucker.pdf.

[2] For a recent study of information disclosure by non-HIPAA-regulated health apps to second, third and even fourth parties, see Quinn Grundy et al., "Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis," *BMJ* 2019;364:l920, http://dx.doi.org/10.1136/bmj.l920, February 25, 2019. The study covers Android health apps, but apps on the iPhone also collect and disclose data without notifying users. Geoffrey A. Fowler, "It's the middle of the night. Do you know who your iPhone is talking to?" *The Washington Post*, May 28, 2019, available at https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/.

[3] See, e.g., Mary Butler, "PHI of Thousands of Mobile Health App Users at Risk in Mobile App Security Breach," Journal of AHIMA, July 11, 2018, available at https://journal.ahima.org/2018/07/11/phi-of-thousands-of-mobile-health-app-users-at-risk-in-mobile-app-security-breach/.

[4] According to the 2019 Verizon Data Breach Investigations Report, "the confluence of design and how users interact with mobile devices make it easier for users to make snap, often uninformed decisions—which significantly increases their susceptibility to social attacks on mobile devices." at https://enterprise.verizon.com/resources/reports/dbir/2019/results-and-analysis/.

[5] Joseph Turow, Michael Hennesy and Nora Draper, "The Tradeoff Fallacy," Annenberg School for Communication, University of Pennsylvania, June 2015, available at https://www.asc.upenn.edu/news-events/publications/tradeoff-fallacy-how-marketers-are-misrepresenting-american-consumers-and.

I suggest that ONC make the following changes to the proposed rule.

- ***Encourage providers to vet or delegate vetting of apps and to set privacy and security requirements for apps***. Vetting would allow providers or their delegates to require apps to have a privacy policy, to disclose what other information an app will collect from the patient's device (e.g., contacts, location, photos, etc.), and to notify patients that data will no longer be protected under HIPAA after it is downloaded. ONC should also permit providers to remove an app from their system not just for malicious behavior but also if an app is found to behave in contravention of its approved privacy policy or is found to be a conduit for inappropriate data acquisition.[6] In recent testimony Dr. Rucker discussed Apple's Health Record app for the iPhone as a success without noting that Apple has strict rules for app developers, including requirements for a privacy policy and special requirements for medical apps.[7] In her testimony at the same hearing, Dr. Kate Goodrich noted that Centers for Medicare & Medicaid Services (CMS) has taken several steps to protect patients who download data through the Blue Button 2.0 program.[8] ONC should not restrict providers from protecting patients at least to the same extent.

  App vetting is not simple or easy.[9] It is encouraging that the proposed rule permits API Technology Suppliers to exercise additional developer vetting as a value-added service. However, the proposed rule sets up barriers to effective vetting. The requirement that vetting be limited to verifying "the authenticity of an application developer" and be completed within five business days (p. 7486, § 170.404(a)(2)(ii)(C)) will severely limit vetting that can be performed, particularly if an application developer is located overseas. The fact that vetting is a value-added service and not a requirement, combined with the warning that such vetting may contravene the Cures Act, makes it more likely that

---

[6] For example, Cambridge Analytica was using data collected as part of a research study for political manipulation. Discovery of such behavior should be sufficient cause to kick an app off a provider's system, even if the app was not hurting the system.

[7] Apple App Store Review Guidelines, https://developer.apple.com/app-store/review/guidelines/, accessed on March 1, 2019.

[8] Statement of Kate Goodrich, M.D, Director, Center for Clinical Standards and Quality, and Chief Medical Officer, Centers for Medicare & Medicaid Services, before the Senate Committee on Health, Education, Labor and Pensions, May 7, 2019, https://www.help.senate.gov/imo/media/doc/Goodrich1.pdf.

[9] For example, the Greater New York Hospital Association's for-profit GNYHA Ventures, created a subsidiary, Happtique, to operate a certification program for health apps. The program was shut down after a CEO of a health IT company found that two of 16 certified apps had serious security issues. Brian Dolan, "Happtique suspends mobile health app certification program," *MobiHealthNews*, December 13, 2013, https://www.mobihealthnews.com/28165/happtique-suspends-mobile-health-app-certification-program/.

incompetent and malicious developers will obtain access to patient health data through marketing or other manipulation. I urge ONC to relax the requirement and permit effective vetting of apps that will have access to EHI.

- ***Prohibit covered entities from offering apps as the only means of data access and export***. Although patients value access to and interaction with their providers' EHRs,[10] there are few statistics on the extent to which patients download their data. I urge ONC to prohibit covered entities from limiting access to patient data only to apps, or from making access via any mechanism other than apps difficult and/or expensive. Consumers have little control over the way apps collect, use and disclose their health data. They should be able to obtain their data in a digital format that does not require giving data to a third party.

- ***Require apps to record metadata for all modifications of the clinical record.*** When I was involved with building PHRs, patient ability to modify records was a barrier to adoption for both patients and providers. Patients did not want to collect and retain medical records if they could not correct errors or at least amend or clarify records before giving them to their next provider. At the same time, providers were concerned that if patients could modify records, the originating organization might be held liable for adverse events resulting from actions taken on the basis of modified records. Nor did receiving providers trust records that may have been modified by patients. A requirement to attach metadata on the clinical side helps address this stalemate, but it is not enough. There is also a need to record metadata on the patient side to enable receiving healthcare organizations to identify data modifications after the record left the originating provider. Since HHS is not in a position to regulate non-HIPAA apps used by patients, this requirement can only be implemented by allowing API Technology Suppliers or providers to require apps to attach metadata to patient actions.

Exceptions to the requirement to disclose data

I commend ONC for not including an expiration date in the patient request to withhold disclosure of their data. Patients shouldn't have to keep track of their requests in order to keep them in force.

I also commend ONC for adopting a standard for data segmentation. The ability to disclose or withhold specific types of health data increases patient trust and willingness to share data. I would urge ONC not to limit the ability of patients and providers to withhold particular data types to the requirements of state and federal law.

---

[10] See, e.g., National Partnership for Women & Families survey, 2014, http://www.nationalpartnership.org/our-impact/news-room/press-statements/new-survey-patients-increasingly-value-electronic-health-records-eager-for-more-access-and-features.html; American Hospital Association annual survey IT supplement, Brief #1, March 2018, https://www.aha.org/system/files/2018-03/expanding-electronic-engagement.pdf.

Some proposed rule provisions on withholding disclosure at the request of the patient are vague and potentially problematic. What constitutes a "legitimate" basis for refusing to disclose information (p. 7532)? For example, in the case of potential spousal abuse, does "legitimacy" require the existence of a police report or some other document? What would constitute "encouragement or inducement by the actor" for a patient request not to share or disclose data? With such ambiguities, it would be easier and less risky for organizations to disclose data and claim that they were required to do so than to try to figure out how to apply the exceptions and sub-exceptions and take on the risk of being accused of information blocking. Once again, I urge ONC to return to the HIPAA Privacy Rule approach that permits but does not require disclosure of data except under specific circumstances.

Disclosures of de-identified data

De-identified data presents a special concern in the regime proposed by ONC, where data disclosure is required unless an exception applies. There is considerable debate within the privacy community about the extent to which accurate re-identification of de-identified data is possible. The computer science community is working on techniques like k-anonymity and differential privacy that can be mathematically proven to provide defined levels of privacy protection through de-identification.[11] I urge ONC to examine work on de-identification with a view to setting standards that would protect patients from having their data re-identified.

Identity and patient record matching

Patient identification is essential for appropriate record matching and appropriate treatment. There are several requirements for inter-organizational matching to be effective. Data must be in standard format. Various organizations must collect data or biometrics that would allow matching with organizations that might have a different set of data or a different preferred matching method. The data set must be difficult for impostors to duplicate. Furthermore, whatever matching method is adopted, it would work best for matching current and future records. Past records, which also have to be matched to the correct patient, may not contain the same data or contain data in the same format. As a result, all patient identification methods, including a unique identifier, have positive and negative aspects.[12]

When examining approaches to patient record matching, ONC should keep in mind that health records have been successfully targeted by identity thieves because they

---

[11] See, e.g., National Academies of Sciences, Engineering, and Medicine. (2017). *Federal Statistics, Multiple Data Sources, and Privacy Protection: Next Steps*. Washington, DC: The National Academies Press. doi: https://doi. org/10.17226/24893.

[12] An extensive discussion of different identification methods and their effects on patient matching can be found in The Pew Charitable Trusts, *Enhanced Patient Matching Is Critical to Achieving Full Promise of Digital Health Records*, October 2018.

are a treasure trove of personal information.[13] ONC should not allow or encourage the collection of so much demographic data for record matching that health records become even more lucrative targets for identity thieves. Extensive collection of demographic information would also facilitate re-identification of de-identified data, which is not subject to the HIPAA Privacy Rule.

In order to effectively deal with identity issues, ONC must differentiate between different uses of identity information.

Identity verification/proofing for enrollment or registration requires a provider to determine whether an identity is real and the individual has a right to claim it. If the wrong individual is enrolled, either through error or subterfuge, the rightful owner of the identity may not be able to prove her claim. Proving that one is the rightful owner of an identity is particularly burdensome if a medical record is tied to biometrics, which are difficult and sometimes impossible to change. Identity proofing must be done not only for the patient but also any delegate who can access the patient's data (e.g., a spouse or legal representative).

ONC notes that identity proofing is essential to protect patient privacy and security (p. 7528). However, identity proofing is not always an explicit legal requirement. When ONC restricts an exemption from disclosure to identity verification required by law (p. 7528) and warns providers not to be too stringent in their identity proofing processes (p. 7536), it subjects patients to increased risk of identity theft. I urge ONC to permit providers to perform whatever identity proofing they deem necessary.

Authentication for data access requires that the individual demonstrate that she has the correct credentials, as issued at enrollment. The authentication process does not require the collection or verification of the same data as enrollment. It is usually limited to knowledge of a shared secret ("something you know," e.g., a password), possession of a token ("something you have," e.g., a phone to receive an access code), or display of a characteristic ("something you are," e.g., a registered biometric). Some additional data may be required for authentication when an authentication token is lost, stolen or is otherwise unusable. I suggest that ONC set limits on how much data can be collected or retained for authentication after identity proofing has been completed.

---

[13] Although some studies indicate that the price of health records has fallen on the black market because the market is saturated (see, e.g., Maria Korolov, "Black market medical record prices drop to under $10, criminals switch to ransomware," December 22, 2016, https://www.csoonline.com/article/3152787/black-market-medical-record-prices-drop-to-under-10-criminals-switch-to-ransomware.html), health records are still more valuable than other types of personal information (see, e.g., Thomas C. Weiss, "The Black Market for Medical and Health Care Records," Disabled World, February, 17, 2015 (Rev. 06/13/2018) available at https://www.disabled-world.com/editorials/technology/blackmarket.php.

Identity elements for patient record matching are different from those used for identity verification/proofing or authentication. Identity matching has become big business for analytics firms, particularly those that want to link individual identities across contexts and devices. ONC should not permit or encourage providers and other organizations to collect excessive amounts of personal data, using record matching as an excuse. ONC should also prohibit the use of identity information from the healthcare context in other contexts, such as marketing.

Data correction: the missing issue

While the ONC proposed rule focuses on data disclosure, it does not mention data correction. In its discussion of sharing misattributed data, ONC heavily favors data sharing and assumes that providers will be able to determine which data is misattributed, segregate such data, and refrain from sharing it while sharing the rest (p. 7524). These are overly optimistic assumptions.

Error propagation in electronic healthcare systems is a significant concern for all system participants because it can have a "cascading effect," corrupting not only the patient's medical record but also claims data, public health data, and data used for research.[14] It is a particular concern for patients because it can lead to incorrect treatment with serious consequences, including death.

Errors in medical records can arise from a variety of sources, such as mix-ups of samples,[15] incorrect data entry, misinterpretation of data taken out of context,[16] or confusion between what a provider prescribed and what the patient actually did.[17] In case of identity theft, an impostor's medical data can become commingled with the data of the real patient in a way that is difficult to disentangle. With increased information sharing, errors can follow the patient as the data is transferred between organizations. For example, one patient who knew that she had been a victim of medical identity theft used a hospital that neither she nor the impostor ever used. The hospital EHR listed the wrong blood type for her because the hospital pulled in data from another hospital that had treated the impostor.[18]

---

[14] Booz Allen Hamilton, "Medical Identity Theft Final Report," January 15, 2009.

[15] See, e.g., CNN, "Breasts Removed By Mistake; Paperwork Slip-Up Blamed," January 21, 2003, http://www.cnn.com/2003/HEALTH/01/20/medical.mistake. A woman had both of her breasts removed after an incorrect diagnosis based on a mix-up of tissue samples.

[16] See, e.g., Lisa Wengsness, "Beth Israel Halts Sending Insurance Data to Google," *The Boston Globe*, April 18, 2009.

[17] Val Jones, MD, "The Costs, And Maybe Cost Savings, Of Medication Non-Adherence," August 28, 2015, Better Health, available at https://getbetterhealth.com/the-costs-and-maybe-cost-savings-of-medication-non-adherence/.

[18] Joseph Menn, "ID Theft Infects Medical Records," *Los Angeles Times*, September 25, 2006, http://pnhp.org/news/id-theft-infects-medical-records/. For a more general discussion of medical identity theft see Pam Dixon, "Medical Identity Theft: An Information Crime That Can Kill You," World Privacy Forum, May 3, 2006.

Data correction is difficult in the current system.[19] HIPAA allows patients to request an amendment of their records, but does not require record holders to accept the request or to change the record.[20] Record holders may refuse to amend a record for various reasons, including fear of liability, suspicion of fraud, or unwillingness to follow the HIPAA requirement to track down and notify other entities that may have received erroneous data.

Unless patients have real ability to correct errors, greater information sharing will increase the risks to patients that providers will act on incorrect information. Attaching metadata to show provenance helps, but it is not enough. I urge ONC to specify that patients must have the right to correct data errors or at least amend their records to ensure that errors do not propagate uncontrollably.

Summary of recommendations

I urge ONC to change the approach in its proposed rule to respect the HIPAA Privacy Rule, which permits but does not require disclosure except to the patient, the Secretary, and in other specific cases. In addition, I recommend the following changes:

- Access and Disclosure
  - Encourage providers to vet or delegate vetting of apps and to set privacy and security requirements for apps
  - Prohibit covered entities from offering apps as the only means of data access and export
  - Require apps to record metadata for all modifications of the clinical record, including those made by the patient after the data is downloaded to an app
  - Clarify proposed rule provisions on withholding disclosure at the request of the patient
  - Examine work on de-identification techniques such as k-anonymity and differential privacy with a view to setting standards that would protect patients from having their data re-identified
- Identity Issues
  - Do not allow or encourage the collection of so much demographic data in the name of record matching that health records become even more lucrative target for identity thieves or facilitate re-identification of de-identified data

---

[19] See, e.g., Dave DeBronkart, "Imagine Someone Had Been Managing Your Data, And Then You Looked." Mr. DeBronkart described in his blog post that it took him months to correct an error that identified his x-ray as belonging to a 53-year-old woman rather than a 59-year-old man. For a more recent experience, see Christina Farr, "This patient's medical record said she'd given birth twice — in fact, she'd never been pregnant," CNBC, December 6, 2018, https://www.cnbc.com/2018/12/09/medical-record-errors-common-hard-to-fix.html.

[20] 45 CFR 164.526.

    - Permit providers to perform whatever identity proofing they deem necessary
    - Limit how much data can be collected or retained for authentication after identity proofing has been completed
    - Prohibit the use of identity information from the healthcare context in other contexts, such as marketing
- Data Correction
    - Specify that patients have the right to correct or at least amend their records to ensure that errors do not propagate uncontrollably

I thank the Department for the opportunity to provide these comments. I would be happy to discuss the comments ONC staff.

Respectfully submitted,

Anna Slomovic, PhD
www.annaslomovic.com