Comments of Anna Slomovic, PhD
Regarding Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans in the Federally- Facilitated Exchanges and Health Care Providers

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

Centers for Medicare & Medicaid Services
Department of Health and Human Services
Attention: CMS-9115-P
Mail Stop C4–26–05
7500 Security Boulevard
Baltimore, MD 21244–1850

Re: RIN 0938–AT79, dated March 4. 2019

I appreciate the opportunity to submit comments on the Centers for Medicare & Medicaid Services (CMS) proposed rule to implement certain provisions of the 21st Century Cures Act. The proposal appears in the *Federal Register*, Vol. 84, No. 42, p. 7610, March 4, 2019.

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. 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.

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 four categories: access to and disclosure of health data; increased surveillance of patients; 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

CMS recognizes that the existence of an open API does not automatically mean that anyone and everyone can connect to it. However, it is disturbing that examples of "acceptable limits [on access to APIs] include technical compatibility and ensuring the application does not pose an unacceptable level of risk to a system when connecting to an API offered by that system." (p. 7620) While system owners are still required to comply with HIPAA and state privacy laws, CMS states that "[a]s noted in guidance from OCR, disagreement with the individual about the worthiness of the third party as a recipient of PHI, or even concerns about what the third party might do with the PHI, are not grounds for denying a request." (p. 7635) It is not clear from this how much control health care entities will be able to exercise over the apps that will extract data from their systems or even how these entities will be able to evaluate the extent of their potential liability under various federal and state laws.

It is even more disturbing that CMS plans to rely on consumer education to mitigate the risk of providing data to non-HIPAA-covered entities. 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]

---

[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

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] A requirement for patient education (p. 7622 and Section III) is not sufficient to ensure that data is not obtained by unscrupulous app developers or disclosed to third and fourth parties in ways that the individual does not understand.

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

- ***Encourage providers and payers 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. CMS should also permit covered entities to remove an app from their system 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

---

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.

[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.

testimony at the same hearing, Dr. Kate Goodrich noted that CMS has taken several steps to protect patients who download data through the Blue Button 2.0 program.[8] CMS should require other covered providers and plans to offer at least that same level of protection.

- ***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,[9] there are few statistics on the extent to which patients download their data. I urge CMS 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.

Increased patient surveillance

It seems that one of CMS's goals is to increase surveillance over patients and, potentially, to increase the pressure on patients to comply with treatment recommendations. ("Identifying and finding opportunities to address the individual's non-adherence to a care plan are critical to keeping people with chronic conditions healthy and engaged so they can avoid hospitalizations." p. 7627) In combination with the requirement to increase data disclosures, this is likely to evolve into more adherence/compliance scoring that can be used by providers, insurers, wellness vendors, and pharmaceutical companies for a variety of purposes.[10] Consumer scoring is completely unregulated outside the credit reporting industry, even though it can have significant effect on the lives of patients and the cost of healthcare.

Similar concerns are raised by proposals to require hospitals to send automatic patient event notifications to various organizations (p. 7650) and to permit

---

[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] 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.

[10] An example of such scoring is FICO's Medication Adherence Score. FICO claims that the score predicts whether a patient will fill prescriptions over the next 12 months. The model utilizes "a wide array of third-party data sources commonly used by direct marketers in a variety of industries," as well as medical or prescription claims data when available. (See https://www.fico.com/en/products/fico-medication-adherence-score) Scores are used to create marketing strategies that target patients and physicians.

transfers of data of multiple patients for overlapping plan/provider populations and plan/plan care coordination (p. 7638). In most of these cases, data recipients are likely to be HIPAA covered entities or their business associates since the transactions are within the healthcare system. Nevertheless, patients will have less control over who has their data. These wide-spread disclosures will also allow data errors to propagate more quickly to more places.

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.[11]

When examining approaches to patient record matching, CMS should keep in mind that health records have been successfully targeted by identity thieves because they are a treasure trove of personal information.[12] CMS 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, CMS 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

---

[11] 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.

[12] 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.

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).

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 CMS set limits on how much data can be collected or retained for authentication after identity proofing has been completed.

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. CMS should not permit or encourage providers and other organizations to collect excessive amounts of personal data, using record matching as an excuse. CMS 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 CMS proposed rule focuses on data disclosure, it does not mention data correction. 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.[13] 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, [14] incorrect data entry, misinterpretation of data taken out of context,[15] or confusion between what a provider prescribed and what the patient actually did.[16] In case of identity theft, an impostor's medical data can become commingled with

---

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

[14] 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.

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

[16] 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/.

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.[17]

Data correction is difficult in the current system.[18] 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.[19] 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 the provenance of clinical data, as proposed by ONC, is helpful but not sufficient. I urge CMS 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.

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

Respectfully submitted,

Anna Slomovic, PhD
www.annaslomovic.com

---

[17] 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.

[18] 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.

[19] 45 CFR 164.526.