

New Rules for Patient Data Sharing Risk Harm to our Most Vulnerable

JESSICA J. POURIAN, MD; DANIEL COGHLIN, MD

KEYWORDS: 21st Century Cures Act, data sharing, adolescent health, confidentiality, health data

Starting this April, patients will be able to access their electronic medical records (EMR) through online patient portals soon after their providers finish their notes. This immediate access will be rolled out as part of the 21st Century Cures Act, a 2016 law passed with broad bipartisan support, which included significant changes for health data sharing. Though some practices have historically allowed patients to see lab results and certain notes, the Cures Act will roll out data access on an unprecedented scale, everywhere. Under the new law, “information blocking,” a practice where a provider prevents or discourages access to health information, becomes illegal.

Giving patients ownership of their data is a noble goal – studies show that patients who are more engaged with their care have improved adherence to medications and better patient-provider communication.¹ Facilitating more patient-provider interactions through online portals has been shown to help address health disparities, especially in patients of color, and to improve patient satisfaction.^{2,3} This is particularly important given that we are in the midst of the COVID-19 pandemic, where telemedicine is increasingly used to manage patient care.

Adolescent data/privacy concerns

However, the new law lacks important nuance on who can access what data and what they can do with it. The Cures Act makes no distinction between adult and pediatric patients, leaving teens in a dangerous grey area. State laws vary dramatically regarding parental access to adolescent data, including whether minors have a right to full confidentiality regarding sexually transmitted infection (STI) screening.⁴ In Rhode Island, minors have a right to confidentiality for STI and pregnancy screening. By default, healthcare data will be accessible to the patient themselves as well as anyone who legally acts on their behalf, such as a caregiver or parent. While a parent accessing the data for the well-child visit of their three-year-old makes sense, the possibility for parents to intrude on the physician-patient relationship for their adolescent children may carry a risk of significant harm. The guarantee of confidentiality has been shown repeatedly

to be one of the most important factors for adolescents seeking healthcare. If teenage patients cannot trust their providers to keep issues of sexual health or substance use – risky behaviors which all peak during adolescence – confidential from their parents, we risk them not disclosing anything at all.⁵ This withholding could have lifelong consequences – a simple chlamydia infection, for example, can lead to permanent infertility if left untreated.⁶ And accidental disclosure for sensitive issues such as gender identity or sexual orientation may cause serious harm to the patient.⁷

We began piloting a note sharing throughout our academic medical center at the end of 2020 in anticipation of the coming changes this spring. Within a month of rollout, we learned that some protected adolescent behavioral health notes were accessed by parents. Upon further investigation, it became clear that many pediatric charts listed the parents’ phone numbers and email addresses as the patients’ contact information, which provided parents with enough information to obtain access to their adolescent children’s portals. With our system sharing notes by default for thousands of kids (in compliance with the impending changes of The Cures Act), it was impossible to distinguish which notes were being sent to the teen versus the parent. As a result, our hospital reached the difficult decision to inactivate all adolescent portal accounts prior to the onset of the Cures Act enforcement date and then offer teens the option to re-enroll in person. This approach provides confirmation that the patient’s phone number and email address are the ones linked to their electronic health information moving forward. This effort has been an enormous logistical challenge. Our institution’s vulnerability to adolescent confidentiality is likely far from unique; we suspect countless other offices and clinics will discover analogous threats as they conform to the information-blocking statutes.

Additional concerns

Adolescents are not the only population at risk from data oversharing. Children in foster care may suddenly find that an estranged biological parent has their new address and healthcare information. Victims of domestic abuse – both children and adults – may face retaliation at home if their abuser sees that violence was discussed in a clinic note. With the Cures Act, all an individual needs is a password to get instant access to extremely sensitive and confidential data.

This is to say nothing of the other elephant in the room – the security risk of a data breach considering the coming EMR integration with third-party applications, which will become more prevalent under the Cures Act. Nationally, there have been repeated data breaches by careless companies and concerted efforts by hackers to access healthcare data. The Cures Act will enable a tremendous flow of health data, yet it provides no regulation for third parties. Mobile app companies have already demonstrated that they need more oversight: it is estimated that 79% of popular health apps routinely share user data, often without informing the patient.⁸ The FDA has not provided any regulations surrounding cybersecurity of healthcare data, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) protections do not apply to third party applications – once that data is out, the patient no longer owns it.

The current wording of the law allows doctors to block release of a specific note or datapoint only if it “prevents harm.” However, this vague wording leaves interpretation up to individual institutions and practitioners, for whom values and incentives may differ. Hospitals may face fines in the millions for instances of information blocking, potentially making it challenging for physicians to advocate for a patient’s privacy on a note-by-note level if hospital policy dictates otherwise. As a result, physicians may self-censor in their notes or water down their conclusions to avoid offending patients in an attempt to preserve the physician-patient relationship.^{9,10} Worries over data sharing may also cause providers to take even longer to write their notes – in institutions where note sharing has already begun, 37% of physicians report spending more time on documentation than before.¹¹

Challenges concerning data privacy within electronic medical records are not new, but the advent the 21st Century Cures Act may bring these difficulties to the forefront of medicine. HIPAA is not enough – we need clearer protections on a national level for our most vulnerable patient populations. National medical societies should move urgently to publish guidance and lobby Congress for patient privacy rights, both for specifics on information blocking and for what third-party apps are permitted to do with health data. We also desperately need technical solutions from our EMR vendors that will enable providers to safeguard patient information without overwhelming us with additional documentation, which contributes disproportionately to physician burnout.¹²

As physicians, we must take care of our patients both in the exam room and in cyberspace. If we cannot remain a trusted, confidential resource, we risk harming our most vulnerable patients. ❖

References

1. Dendere R, Slade C, Burton-Jones A, Sullivan C, Staib A, Janda M. Patient portals facilitating engagement with inpatient electronic medical records: A systematic review. *J Med Internet Res.* 2019;21(4).
2. Gerard HC. The Importance of Visit Notes on Patient Portals for Engaging Less Educated or Nonwhite Patients: Survey Study. *J Med Internet Res.* 2018;20(5):191.
3. Walker J, Leveille S. OpenNotes After 7 Years: Patient Experiences With Ongoing Access to Their Clinicians’ Outpatient Visit Notes. *J Med Internet Res.* 2019;21(5).
4. Guttmacher Institute. An Overview of Consent to Reproductive Health Services by Young People. Published October 2020. Accessed October 11, 2020. <https://www.guttmacher.org/state-policy/explore/overview-minors-consent-law#>
5. Ford CA, English A. Limiting confidentiality of adolescent health services: What are the risks? *J Am Med Assoc.* 2002;288(6):752-753.
6. Murray PJ, Braverman PK, Adelman WP, et al. Screening for nonviral sexually transmitted infections in adolescents and young adults. *Pediatrics.* 2014;134(1):302-311.
7. McGeough BL, Sterzing PR. A Systematic Review of Family Victimization Experiences Among Sexual Minority Youth. *J Prim Prev.* 2018;39(5):491-528.
8. Grundy Q, Chiu K, Held F, Continella A, Bero L, Holz R. Data sharing practices of medicine-related apps and the mobile ecosystem: Traffic, content, and network analysis. *BMJ.* 2019;364:920.
9. Blease C, O’Neill S, Walker J, Hagglund M. Sharing notes with mental health patients: balancing risks with respect. *The Lancet Psychiatry.* 2020;7(11):924-925.
10. Dobscha S, Denneson L. VA mental health clinician experiences and attitudes toward OpenNotes. *Gen Hosp Psychiatry.* 2016;38:89-93.
11. DesRoches C, Leveille SB. The Views and Experiences of Clinicians Sharing Medical Record Notes With Patients. *JAMA Netw.* 2020;3(3).
12. Ehrenfeld JM, Wanderer JP. Technology as friend or foe? Do electronic health records increase burnout? *Curr Opin Anaesthesiol.* 2018;31(3):357-360.

Authors

Jessica J. Pourian, MD, PGY-1, Department of Pediatrics, Warren Alpert Medical School of Brown University, Providence, RI.
Daniel Coghlin, MD, Associate Professor, Clinician Educator, Department of Pediatrics, Warren Alpert Medical School of Brown University, Providence, RI.

Correspondence

Jessica J. Pourian, MD
Department of Pediatrics
593 Eddy St.
Providence, RI 02903
jessica_pourian@brown.edu