Privacy Risks of Interoperable Electronic Health Records: Segmentation of Sensitive Information Will Help

Currents in Contemporary Bioethics

Mark A. Rothstein and Stacey A. Tovino

At the turn of this century, as the United States began shifting from paper to electronic health records (EHRs), the new records were touted as promoting improved care, efficiency, patient safety, and patient participation in their own health management. EHRs were said to have several highly valuable characteristics, including that they are comprehensive (capturing substantially all of a patient's clinical encounters in the health care system), longitudinal (capturing health information from cradle to grave), and interoperable (permitting access for viewing and uploading new information from multiple locations).[1]

The promise of interoperability was a significant justification for the effort to switch from paper records to EHRs. Interoperability meant that (1) patients, caregivers, and providers would be relieved of the burden of providing or obtaining repetitive health histories for each new patient-provider relationship; (2) costly and onerous duplicative tests, imaging, and diagnostic procedures need not be repeated; (3) more efficient coordination of care and health benefits would be possible; and (4) complete health records for treatment in emergencies could be accessed in real time from distant locations.[2]

By 2015, encouraged by $35 billion in federal financial incentives from the Health Information Technology for Economic and Clinical Health Act (HITECH Act),[3] 78 percent of physicians[4] and 96 percent of hospitals[5] had an EHR system certified by the Department of Health and Human Services (DHHS). Although EHRs were, to a degree, comprehensive and longitudinal, they were generally not interoperable, owing to incompatible software, access "blocking" to protect the proprietary interests of EHR vendors and health care providers, and the federal government having other regulatory priorities.

By 2019, federal regulatory priorities had shifted, and the Centers for Medicare and Medicaid Services (CMS) of DHHS published a proposed rule to establish standards for interoperability.[6] As discussed below, the proposal goes into great detail about the technical aspects of interoperability under various federal statutes and programs. Nevertheless, the proposed rule astoundingly fails to address the significant risks to health privacy posed by interoperable EHRs. This article analyzes one of the key privacy risks, interoperable comprehensive records.

Key Provisions of the Proposed Rule

Published in the *Federal Register* on March 4, 2019, CMS's Interoperability and Patient Access Proposed Rule (Proposed Rule) requests information, solicits public comment, and proposes to implement a number of requirements that apply in whole or in part to Medicare Advantage (MA) organizations, state Medicaid and Children's Health Insurance Program (CHIP) fee-for-service (FFS) programs, Medicaid managed care plans, CHIP managed care entities, Qualified Health Plan (QHP) issuers in Federally-Facilitated Exchanges (FFEs), and certain health care providers.[7] The Proposed Rule may be divided into nine substantive sections relating to: (1) the implementation, testing, and monitoring of application program interface technology;[8]

About This Column

Mark A. Rothstein serves as the section editor for *Currents in Contemporary Bioethics.* Professor Rothstein is the Herbert F. Boehl Chair of Law and Medicine and the Director of the Institute for Bioethics, Health Policy and Law at the University of Louisville School of Medicine in Kentucky. (mark.rothstein@louisville.edu)

Mark A. Rothstein, J.D., *is the Herbert F. Boehl Chair of Law and Medicine and Director of the Institute for Bioethics, Health Policy and Law at the University of Louisville School of Medicine.* **Stacey A. Tovino, J.D., Ph.D.,** *is the Judge Jack and Lulu Lehman Professor of Law at the University of Nevada, Las Vegas, William S. Boyd School of Law.*

The Journal of Law, Medicine & Ethics, 47 (2019): 771-777. © 2019 The Author(s)
DOI: 10.1177/1073110519897791
https://doi.org/10.1177/1073110519897791 Published online by Cambridge University Press

(2) required participation in trusted exchange networks;[9] (3) an increase in the frequency of federal-state data exchanges;[10] (4) public reporting of providers' "negative attestations" to "information blocking prevention";[11] (5) public reporting of missing provider digital contact information;[12] (6) "electronic patient event notifications"[13] by general hospitals, psychiatric hospitals, and critical access hospitals;[14] (7) the advance of interoperability across the health care continuum;[15] (8) the advance of interoperability in innovative models;[16] and (9) policies to improve patient matching.[17] Illustrative requests, solicitations, and proposals that raise privacy and security concerns are discussed in more detail below.

Implementation, Testing, and Monitoring of API Technology

In the last decade CMS has launched several initiatives designed to improve patient access to health information. In 2010, for example, CMS established the initial Medicare Blue Button service, enabling Medicare FFS beneficiaries to download their Parts A, B, and D health care claims data through MyMedicare.gov in either pdf. or text format.[18] Eight years later, CMS launched its Blue Button 2.0 application programming interface (API), also in Medicare FFS.[19] An API allows software from different developers to connect with one another and to exchange electronic health information in formats that can be easily compiled, accessed, and used by patients and their caregivers.[20] Blue Button 2.0 specifically allows: (1) an application developer to register a beneficiary-facing application; and (2) a beneficiary to grant that application access to four years of the beneficiary's Medicare Parts A, B, and D claims data. As a result of Blue Button 2.0, Medicare FFS beneficiaries will be able to download[21] their Medicare health information along with their other health information into a single application not dictated by any specific health plan, provider, or portal.[22]

CMS's Proposed Rule builds on Blue Button 2.0 by requiring MA organizations, state Medicaid and CHIP FFS programs, Medicaid managed care plans, CHIP managed care entities, and QHP issuers in FFEs (excluding issuers of stand-alone dental plans (SADPs)) to implement, test, and monitor an openly-published API that is accessible to third-party applications and developers.[23] The API would allow enrollees and beneficiaries of these organizations, programs, and plans to exercise electronically their right to access plan-specific protected health information (PHI) as required by the HIPAA Privacy Rule[24] through the use of common technologies (e.g., computers, smartphones, tablets) but without special effort and without advanced technical skills.[25] Under the Proposed Rule, the information to be made accessible through the open API includes adjudicated claims data, provider remittances, enrollee cost-sharing, capitated provider encounters, and clinical data, including laboratory results.[26]

Participation in Trusted Exchange Networks

The Proposed Rule also would require MA plans, Medicaid managed care plans, CHIP managed care entities, and QHPs in the FFEs (excluding SADP issuers) to participate in a trusted exchange network.[27] A trusted exchange network involves a common set of principles designed to facilitate trust among disparate health information networks (HINs) and by which all HINs should abide in order to enable widespread electronic health data exchange. According to CMS, widespread payer participation in trusted exchange networks might allow for more complete access to and exchange of electronically accessible health information between and among providers and plans, which might lead to better use of such data.[28] Under the Proposed Rule, the trusted exchange network in which participation is required must: (1) be capable of exchanging PHI in compliance with all applicable federal and state laws; (2) be capable of connecting to inpatient EHRs and ambulatory EHRs; and (3) support secure messaging or electronic querying by and between providers, payers, and patients.[29]

Increase in the Frequency of Federal-State Data Exchanges

The Proposed Rule also strives to improve the experience of individuals who are dually eligible for Medicare and Medicaid.[30] Medicare and Medicaid are distinct programs with different purposes and different governing rules.[31] For example, Medicare and Medicaid have different standards for eligibility, different covered benefits, and different provider payments.[32] Nevertheless, a growing number of individuals are eligible for, and depend on, both programs for their health care.[33] In the preamble to the Proposed Rule, CMS expressed its belief that there is an increasing need to align Medicare and Medicaid, including the data and systems that support these programs, to improve not only care delivery but the overall experience of individuals who are dually eligible.[34] Although the states and CMS already exchange data to support the administration of benefits to individuals who are dually eligible for both programs, including "buy-in" data on who is enrolled in Medicare and who is liable for paying the beneficiary's Part A and B premiums,[35] the Proposed Rule would increase the frequency of federal and state data exchanges from a monthly exchange to a daily (i.e., every business day) exchange.[36] CMS believes that the current, month-long lag in updating buy-in data precludes states from terminating or activating buy-in coverage sooner, which can result in the state or beneficiary paying premiums for longer than appropriate.[37]

Increase in Electronic Patient Event Notifications

In addition to the payer-focused proposals described above, the Proposed Rule also seeks to amend the Conditions of Participation (COPs) applicable to Medicare-participating hospitals, psychiatric hospitals, and critical access hospitals (CAHs).[38] The COPs establish, among other standards, basic health and safety standards that govern the transition of discharged hospital patients to other settings.[39] The Proposed Rule would require Medicare-participating hospitals, psychiatric hospitals, and CAHs to

https://doi.org/10.1177/1073110519897791 Published online by Cambridge University Press

send certain "electronic patient event notifications"[40] to certain practitioners and certain service providers when a patient is admitted, discharged, or transferred if the hospital, psychiatric hospital, or CAH uses an electronic medical records system that has the capacity to generate patient event notifications.[41] Under the Proposed Rule, each notification must include the following information: "patient name, treating practitioner name, sending institution name, and, if not prohibited by other applicable law, patient diagnosis."[42]

Information Requests; Comment Solicitations

The Proposed Rule also requests information and solicits comments on several issues that have significant privacy and security implications. With respect to unique patient identifiers (UPIs), for example, CMS explained that it "understands the significant health information privacy and security concerns raised around the development of a UPI standard and the current prohibition against using HHS funds to adopt a UPI standard."[43] Nevertheless, CMS is seeking public comment on ways the Office of the National Coordinator for Health Information Technology (ONC) and CMS can continue to facilitate private sector efforts on a workable and scalable patient matching strategy so that the lack of a UPI does not impede the free flow of information.[44]

With respect to the advance of interoperability across the care continuum, CMS explained that poor patient outcomes, resulting from poor communication and lack of information, have been found to contribute to hospital readmissions, emergency department visits, and adverse outcomes.[45] CMS further stated that a well-documented contributor to this problem is incomplete and missing information for patients with frequent transitions across care settings.[46] "While interoperable, bidirectional exchange of essential health information can improve these transitions, many long-term and post-acute care (PAC), behavioral health, and home and community-based service providers have not adopted health IT at the same rate as acute care hospitals."[47] To this end, CMS seeks comment on: (1) how DHHS can more broadly incentivize the adoption of interoperable health IT systems and use of interoperable data across settings, such as long-term care, PAC, behavioral health, and home and community-based services;[48] and (2) whether hospitals and physicians should be capable of electronically exchanging a subset of the PAC standardized patient assessment data elements (e.g., functional status, pressure ulcers, injuries) through their EHRs.[49]

The Proposed Rule increases privacy and security risks involving identifiable patient data. One way in which this would occur is that the Proposed Rule increases both the volume of data exchanged as well as the frequency with which data are exchanged.

Increased Privacy Risks

The Proposed Rule increases privacy and security risks involving identifiable patient data. One way in which this would occur is that the Proposed Rule increases both the volume of data exchanged as well as the frequency with which data are exchanged. Recall that the data to be made available through the proposed open API includes data about adjudicated claims, provider remittances, enrollee cost-sharing, capitated provider encounters, and clinical data, including laboratory results. In addition, the information that must accompany each proposed transition notification by a hospital, psychiatric hospital, or CAH includes the patient's name, the treating practitioner's name, the sending institution's name, and, unless prohibited by other law, the patient's primary diagnosis. Moreover, the data that would be exchanged on a daily versus monthly basis to improve the experience of individuals dually eligible for Medicare and Medicaid includes files of all eligible Medicaid beneficiaries by state as well as "buy-in" data. By increasing the amount of data exchanged and the frequency of such exchanges, these proposals increase the risk that, in the case of a data breach or other unauthorized disclosure of identifiable patient data, more data would be released that could increase harm to individuals

The Proposed Rule also intensifies concerns relating to user authentication, "access control,"[50] and personal representatives, among other issues. The identity of enrollees who will have access to their comprehensive, longitudinal EHRs must be properly verified; otherwise, cradle-to-grave data will be fully accessible to unauthorized users. Access controls must be properly established and implemented; otherwise, verified enrollees may be able to access other enrollees' data. When a living enrollee has a properly designated personal representative, or when the personal representative of an estate or other person has authority to act on behalf of a deceased enrollee, the personal representative must have proper access to information that is relevant to the representation but not access to information beyond the scope of the representation.

CMS appears to recognize that privacy and security risks are associated with some of its proposals, but its focus is mostly on security. For example, CMS referenced in the preamble to the Proposed Rule the number of breach incidents that occurred during the first three quarters of 2018 together with the fact that these breach incidents affected more than 4.3 million individuals.[51] CMS also

https://doi.org/10.1177/1073110519897791 Published online by Cambridge University Press

stated in the preamble that, "Ensuring the privacy and security of the claims encounter, and other health information when it is transmitted through the API is of critical importance."[52] Within its proposed API regulation, CMS specifically requires each payer to "conduct routine testing and monitoring to ensure the API functions properly, including assessments to verify that the API is fully and successfully implementing privacy and security features [as required by the HIPAA Privacy Rule and 42 C.F.R. Part 2]."[53] Finally, CMS requested comment on whether existing privacy and security standards, including the HIPAA Privacy and Security Rule, are sufficient or whether CMS should develop additional privacy and security standards to accompany its proposals.[54]

Need for Patient Control of Sensitive Information

Although the implementation of interoperability languished, proposals to protect health privacy were publically debated and included in several key documents. In 2009, the HITECH Act directed the Health Information Technology Policy Committee at DHHS (established by the HITECH Act) to make recommendations for:

> the segmentation and protection from disclosure of specific and sensitive individually identifiable health information with the goal of minimizing the reluctance of patients to seek care (or disclose information about a condition) because of privacy concerns ...[55]

From 2013-2015, ONC supported the development of a technical standard to implement this provision. Termed Data Segmentation for Privacy (DS4P),[56] it involved adding a metadata tag to health information requiring additional patient consent before disclosure. Both technical solutions and policy development are essential for privacy protection with interoperable health records, and both aspects are lagging today.

With regard to policy, proposals for segmentation predate the HITECH Act. They were originally proposed by the National Committee on Vital and Health Statistics (NCVHS), the statutory public advisory committee to the Secretary of DHHS on health data, statistics, privacy, and national health information policy.[57] NCVHS held a series of public hearings and obtained testimony from a wide range of health care providers, patient advocacy organizations, technology experts, and members of the public. It then deliberated and wrote detailed letter reports to the Secretary in 2006, 2008, and 2010, in which it proposed measures to protect patient privacy in an environment of interoperable EHRs.[58]

A key element of these proposals by the NCVHS was to allow individuals to "segment" sensitive information in their health records based on a limited number of predefined categories. This was a middle ground position between the status quo of not permitting patients to control their health records and allowing patients to direct the deletion of information from their records. Any deletions would violate state medical record laws, and this option also was strongly opposed by clinicians who recoiled at the notion of caring for patients based on patients' selectively edited health records. Under the NCVHS proposal, health information that was segmented in EHRs would not be accessible to health care providers for treatment without additional consent. Segmented information also would not be disclosed to a third party (e.g., employer, life insurer) pursuant to a general authorization. Besides the enhanced privacy protection afforded by segmentation, the NCVHS noted the public health significance of this measure.

> [T]here is a strong public interest in encouraging individuals to seek prompt treatment for sensitive health conditions, such as domestic violence, sexually transmitted diseases, substance abuse, and mental illness. If individuals fear that they have no control over such sensitive health information or that they cannot trust that their sensitive health information will be protected from unwanted disclosure, they might fail to divulge sensitive information relevant to their care, fabricate answers to sensitive questions, or even avoid seeking timely health care altogether, thereby endangering their own health, and possibly the health and safety of others.[59]

The NCVHS also pointed out, based on testimony at public hearings, that in countries such as Denmark, which permits patients to restrict the disclosure of all sensitive information in their health records, people rarely elected to do so, but they strongly valued the ability to do so.[60]

In considering the adoption of a policy authorizing segmentation, the first question to resolve is what categories of information should be eligible for segmentation. In its 2010 letter, the NCVHS wrote that the categories could include health information already recognized by federal law for separate treatment, including genetic information (pursuant to the Genetic Information Nondiscrimination Act (GINA)),[61] psychotherapy notes (excluded from routine disclosure pursuant to the HIPAA Privacy Rule),[62] and substance use treatment records (pursuant to the Public Health Service Act and regulations of the Substance Abuse and Mental Health Services Administration).[63] In addition, the NCVHS included categories already designated by the laws in some states or otherwise qualifying for special confidentiality protections, including HIV/AIDS information, mental health information, health records of children and adolescents, information about sexuality and reproductive health, information about domestic violence or stalking, and information about an individual whose identity needed protection.[64]

Besides selecting and precisely defining the categories of information eligible for segmentation, there

https://doi.org/10.1177/1073110519897791 Published online by Cambridge University Press

The inability of health care providers and patients to access, aggregate, and use complete health records has been a significant drawback of both paper and electronic health records. Yet, the unintentional compartmentalization of sensitive health information has served to protect health privacy. Interoperability, a fundamental aspect of EHR systems, may soon be achievable in light of the recently proposed DHHS rule. Unfortunately, the proposal focuses largely on the benefits of and technical challenges in achieving interoperability. It fails to convey a sense of urgency needed to address the serious health privacy consequences of comprehensive and longitudinal records.

are numerous issues to be resolved, including the following:

1. What, if any, notice should be given to health care providers to alert them that the records have been segmented? The NCVHS considered it important to notify providers that the EHR was incomplete so that, if necessary, additional consent could be sought. The NCVHS recommended that the notation be general and not indicate the category of information segmented, because disclosing, for example, that mental health information had been segmented would destroy much of the privacy value of segmentation.
2. What additional consent should be needed to access segmented health information? The NCVHS proposed that all disclosures of segmented health information should be noted in the EHR, along with the additional consent that would permit access to the segmented information.
3. Should health care providers have access to complete health records in an emergency? The NCVHS recommended that a "break the glass" feature should be a part of segmentation, but there should be a notation of when, why, and by whom this was done, along with the measures taken to "re-segment" the information when no longer needed.
4. Should clinical decision support be able to scan segmented information? The NCVHS thought this was important for patient care. For example, a confirmed diagnosis of a segmented health condition would be valuable to a health care provider in making a diagnosis of a separate condition. It might also prevent repetitive imaging or other diagnostic tests[65]

Conclusion

The inability of health care providers and patients to access, aggregate, and use complete health records has been a significant drawback of both paper and electronic health records. Yet, the unintentional compartmentalization of sensitive health information has served to protect health privacy. Interoperability, a fundamental aspect of EHR systems, may soon be achievable in light of the recently proposed DHHS rule. Unfortunately, the proposal focuses largely on the benefits of and technical challenges in achieving interoperability. It fails to convey a sense of urgency needed to address the serious health privacy consequences of comprehensive and longitudinal records.

Options to protect privacy in interoperable health records have been carefully considered by scholars, policy analysts, and experts in health information technology. The NCVHS recommended a system whereby individuals would be permitted to select one or more predefined categories of health information for segmentation. Adopting such a policy will require a willingness to change the way medical records traditionally have been generated and used. Failing to take such action, however, will expose individuals to great and continuing privacy risks from routine disclosures of sensitive health information. It will also undermine the accuracy of health records, as patients will most assuredly engage in self-help measures to protect their privacy by not disclosing certain information to their providers in the first instance.

Other important privacy issues are raised by the Proposed Rule. Of great significance is the notion that individuals will be able to access their complete records by downloading them using a new app on their mobile devices. There are numerous privacy issues raised by the use of health apps on mobile devices (e.g., third-party access),[66] and there was no mention of these issues in the Proposed Rule. Interoperability is the last major element of a new EHR system, and therefore it may be the last opportunity to protect health privacy through uniform design standards.

Acknowledgements

The authors thank Maya Bernstein for her valuable comments on an earlier draft, but they are solely responsible for the content.

https://doi.org/10.1177/1073110519897791 Published online by Cambridge University Press

Note

The authors have no conflicts to declare.

References

1. *See generally* Institute of Medicine, *Crossing the Quality Chasm: A New Health System for the 21st Century* (Washington, DC: National Academy Press, 2001); D. Merritt, ed., *Paper Kills: Transforming Health and Health Care with Information Technology* (Washington, DC: CHT Press, 2007).
2. Markle Foundation, *Connecting Americans to their Healthcare: A Common Framework for Networked Personal Health Information* (2006), *available at* <http:www.connectingforhealth.org/commonframework/docs/p9_networkedphrs.pdf> (last visited November 18, 2019).
3. Pub. L. 111-5 (February 17, 2009), 42 U.S.C. § 300jj et seq.
4. Office of the National Coordinator for Health Information Technology, *Health IT Dashboard,* "Office-based Physician Health IT Adoption: State Rates of Physician EHR Adoption, Health Information Exchange and Interoperability, and Patient Engagement (2015)," *available at* <https://dashboard.healthit.gov/apps/physician-health-it-adoption.php> (last visited November 18, 2019).
5. Office of the National Coordinator for Health Information Technology, *Health IT Dashboard,* "Non-federal Acute Care Hospital Health IT Adoption and Use: State Rates of Non-federal Acute Care Hospital EHR Adoption, Health Information Exchange and Interoperability, and Patient Engagement (2015), *available at* <https://dashboard.healthit.gov/apps/hospital-health-it-adoption.php> (last visited November 18, 2019).
6. Centers for Medicare and Medicaid Services, Department of Health and Human Services, Proposed Rule, 84 Fed. Reg. 7610-7680 (March 4, 2019).
7. 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, 84 Fed. Reg. 7610, 7610-7680 (proposed Mar. 4, 2019) (to be codified at 42 C.F.R. Parts 406, 407, 422, 423, 431, 438, 457, 482, and 485; and 45 C.F.R. Part 156) [hereinafter Proposed Rule].
8. 84 Fed. Reg.. at 7618-7639 (preamble discussion of the proposed API requirement).
9. *Id.* at 7642-7643 (preamble discussion of the proposed trust network participation requirement).
10. *Id.* at 7643-7645 (preamble discussion regarding the frequency of federal-state data exchanges).
11. *Id.* at 7645-7648 (preamble discussion of the proposed public reporting of providers' negative attestations to the prevention of information blocking); *id.* at 7647 ("We believe … the Affordable Care Act provides the statutory authority to publicly report certain data about the prevention of information blocking attestation statements as an assessment of care coordination …"; *id.* at 7618 ("[W]e are proposing to publicly post information about negative attestations on appropriate CMS websites.").
12. *Id.* at 7648-7649 (preamble discussion of the proposed public reporting of missing provider digital contact information).
13. *Id.* at 7650 ("Electronic patient event notifications from hospitals, or clinical event notifications, are one type of health information exchange intervention that has been increasingly recognized as an effective and scalable tool for improving care coordination across settings, especially for patients at discharge").
14. *Id.* at 7649-7653 (preamble discussion of the proposed revisions to the Medicare Conditions of Participation applicable to hospitals, psychiatric hospitals, and critical access hospitals relating to electronic patient event notifications of a patient's admission, discharge, and/or transfer to another health care facility or another health care provider).
15. *Id.* at 7653-7655 (preamble discussion of, and solicitation of comments regarding, the advance of interoperability between and among post-acute care (PAC), long term, behavioral health, and home and community-based service providers).
16. *Id.* at 7655-7656 (preamble discussion of, and solicitation of comments regarding, the advance of interoperability through innovative models).
17. *Id.* at 7656-7657 (preamble request for information regarding how CMS can leverage its authority to improve patient identification through improved patient matching).
18. *Id.* at 7626 (discussing the 2010 Medicare Blue Button initiative).
19. Centers for Medicare and Medicaid Services, Blue Button 2.0, *available at* <https://bluebutton.cms.gov/> (last visited November 18, 2019) [hereinafter Blue Button 2.0].
20. Proposed Rule, *supra* note 7, at 7626.
21. *Id* ("One benefit of making records available via an API is that it enables a beneficiary to pull Medicare health information along with other heath information into a single application not dictated by any specific health plan, provider, or portal.").
22. *Id.*
23. *Id.* at 7674-7680 (proposing new API regulations to be codified within 42 C.F.R. Parts 422, 431, and 457 as well as within 45 C.F.R. Part 156).
24. 45 C.F.R. § 164.524(a)(1) (2018) ("[A]n individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set …").
25. Proposed Rule, *supra* note 7, at 7627-7628 ("The API would allow enrollees and beneficiaries … to exercise electronically their HIPAA right of access to certain health information specific to their plan, through the use of common technologies and without special effort.").
26. *See, e.g., id.* at 7628 (preamble discussion thereof); *id.* at 7675 (proposing new 42 C.F.R. § 431.60(b)) (listing these required content elements).
27. *See, e.g., id.* at 7642-7643 (preamble discussion of the proposed trust network participation requirement); *id.* at 7675 (proposing new 42 C.F.R. § 422.119(f)(2) applicable to MA plans); *id.* at 7676 (proposing new 42 C.F.R. § 438.242(b)(5) applicable to Medicaid and CHIP managed care plans); *id.* at 7680 (proposing new 45 C.F.R. § 156.221(f)(2) applicable to QHPs in FFEs).
28. *Id.* at 7642.
29. *Id.* at 7675 (proposing new 42 C.F.R. § 422.119(f)(2)(i)-(iii)); *id.* at 7676 (proposing new 42 C.F.R. § 438.242(b)(5)(i)-(iii)); and *id.* at 7680 (proposing new 45 C.F.R. § 156.221(f)(2)(i)-(iii)).
30. *Id.* at 7643.
31. *Id.*
32. *Id.*
33. *Id.*
34. *Id.*
35. *Id.* at 7618 (explaining that "buy-in" data are data showing who is enrolled in Medicare and who is liable for paying for a dual eligible beneficiary's Medicare Part A and Part B premiums; further explaining that buy-in data exchanges support state, CMS, and Social Security Administration premium accounting, collections, and enrollment functions).
36. *Id.* at 7643.
37. *Id.*
38. The Medicare Conditions of Participation applicable to hospitals, psychiatric hospitals, and critical access hospitals are codified at 42 C.F.R. Parts 482 and 485.
39. *See, e.g.,* 42 C.F.R. § 482.43 (regulating Medicare-participating hospital discharge planning).
40. *Id.* at 7618 (discussing electronic patient event notifications).
41. Proposed Rule, *supra* note 7, at 7678 (proposing new 42 C.F.R. §§ 482.24(d) and 482.61(f)); *id.* at 7679 (proposing new 42 C.F.R. § 485.638(d)).
42. *Id.*
43. *Id.* at 7615.
44. *Id.*
45. *Id.* at 7654.
46. *Id.*
47. *Id.*
48. *Id.*

https://doi.org/10.1177/1073110519897791 Published online by Cambridge University Press

[49] *Id.* at 7655.

[50] "Access control" refers to policies and procedures that allow ePHI access only to those persons or software programs that have been granted access rights. *See, e.g.*, 45 C.F.R. § 164.312(a).

[51] Proposed Rule, *supra* note 7, at 7615.

[52] *Id.* at 7635.

[53] *See, e.g., id.* at 7674 (proposing new 42 C.F.R. § 422.119(c)(2)).

[54] *Id.* at 7635.

[55] HITECH Act § 3002(b)(2)(B)(i), 42 U.S.C. § 300jj-12.

[56] Office of the National Coordinator for Health Information Technology, 2015 Edition of Final Rule: Data Segmentation for Privacy (DS4P), HealthIT.gov, *available at* <https:www.healthit.gov/sites/default/files/2015editionehrcertificationcriteriads4p10615.pdf> (last visited November 18, 2019).

[57] National Committee on Vital and Health Statistics, *available at* <www.ncvhs.hhs.gov> (last visited November 18, 2019).

[58] Co-author Mark A. Rothstein was a member of the NCVHS from 1999-2008 and chaired its Subcommittee on Privacy and Confidentiality, which conducted the hearings and wrote the initial drafts of the letters described. Because his term ended in 2008, he did not take part in drafting the 2010 letter.

[59] National Committee on Vital and Health Statistics, Letter to Michael O. Levitt, Secretary of Health and Human Services, February 20, 2008, at 3, *available at* <https://ncvhs.hhs.gov/wp-content/uploads/2014/05/080220lt.pdf> (last visited November 18, 2019).

[60] *Id.*

[61] Pub. L. 110-223 (2008).

[62] 45 C.F.R. § 164.508(a)(2).

[63] 42 U.S.C. § 290dd-2; 42 C.F.R. Part 2.

[64] National Committee on Vital and Health Statistics, Letter to Kathleen Sebelius, Secretary of DHHS, November 10, 2010, at 7-14, *available at* <https://ncvhs.hhs.gov/wp-content/uploads/2014/05/101110lt.pdf> (last visited November 18, 2019).

[65] NCVHS Letter of February 20, 2008, *supra* note 10. *See generally* M.A. Rothstein, "Access to Sensitive Information in Segmented Electronic Health Records," *Journal of Law, Medicine & Ethics* 40, no. 2 (2012): 394-400; M.A. Rothstein, "Health Privacy in the Electronic Age," *Journal of Legal Medicine* 28, no. 2 (2007): 487-501, 496-497.

[66] *See* M.A. Rothstein et al., "Unregulated Health Research Using Mobile Devices: Ethical Considerations and Policy Recommendations," *Journal of Law, Medicine & Ethics* 48, no. 1 (Supp.) (2020): forthcoming.

The Journal of Law, Medicine & Ethics, 47 (2019): 771-777. © 2019 The Author(s)

https://doi.org/10.1177/1073110519897791 Published online by Cambridge University Press