DePaul Law Review

Volume 68
Issue 2 *Winter 2019*

Article 2

How to Safely Make Interoperable Health Information Exchange a Reality

Julia Adler-Milstein

HOW TO SAFELY MAKE INTEROPERABLE HEALTH INFORMATION EXCHANGE A REALITY

*Julia Adler-Milstein**

I. The Benefits and Risks of Health Information Technology Use at the Point-of-Care

Health information technology to support frontline clinical care carries enormous potential for benefit but also risks if used improperly (most often, unintentionally). Particularly in the patient safety domain, there is little disagreement that shifting from a largely paper-based approach to documenting care, to an electronic record keeping system in which clinical decisions can be supported by smart tools, would produce safer care and better outcomes.[1] There is evidence to support important safety gains from health IT—particularly from clinical decision-support systems to avoid adverse drug events[2]—but there is also evidence that reveals the new types of patient safety risks introduced by health IT.[3] While the causes of such unintended consequences are varied, two primary causes are: (1) an under-appreciation of the complexity of integrating health IT tools into care delivery and (2) an environment in which policies, incentives, and regulations produce stakeholder interests that are not always aligned behind the goal of translating health IT tools into safer care.

II. Interoperable Electronic Health Information Exchange and Expected Benefits

Interoperable electronic health information exchange (HIE) is a critical domain in which there are significant potential benefits along-

* Associate Professor, Department of Medicine, University of California, San Francisco. This Article is based on collaborative work with Carol Parker, Michelle Mello, Lucia Savage, & Martin Gaynor.

1. Janet M. Corrigan et al., Crossing the Quality Chasm: A New Health System for the 21st Century 4, 15–16 (2001).

2. Michael F. Furukawa et al., *Meaningful Use of Health Information Technology and Declines in In-Hospital Adverse Drug Events*, 24 J. Am. Med. Informatics Ass'n 729, 729–33, 735 (2017); Rainu Kaushal et al., *Effects of Computerized Physician Order Entry and Clinical Decision Support Systems on Medication Safety: A Systematic Review*, 163 Archives Internal Med. 1409, 1409–10, 1413–14 (2003).

3. James M. Walker et al., *EHR Safety: The Way Forward to Safe and Effective Systems*, 15 J. Am. Med. Informatics Ass'n 272, 272–74 (2008).

side potential associated harms from making care less safe (i.e., an unintended consequence) or preventing care from getting safer (i.e., lack of intended benefits realization). As an IT-enabled solution, HIE seeks to ensure that health information can follow patients across care delivery settings, such that their providers have complete information.[4] Missing patient information occurs frequently and manual processes of information exchange introduce patient safety risks (e.g., handwriting errors).[5] Therefore, widespread electronic health record (EHR) adoption coupled with HIE is expected to improve patient outcomes and is currently a top policy priority.[6]

More specifically, the benefits of HIE are many because, in concept, HIE should enable access to complete patient information at the point-of-care.[7] This should avoid care that is duplicative and potentially unsafe. The empirical evidence to-date suggests reductions in redundant care as a result of HIE, primarily reductions in laboratory and imaging tests.[8] Reducing unnecessary imaging, and the associated exposures known to harm patients, is therefore the domain with the best evidence for how HIE is likely to improve patient safety. However, more complete information enabled by HIE should result in a range of other patient safety benefits, such as more accurate diagnoses and a reduction in potentially harmful drug-drug interactions, drug-allergy interactions, and drug-lab interactions.[9] While these gains are important, rapid expansion of HIE across disparate EHRs also holds the potential to introduce new types of patient safety errors that are not well understood. This will likely require legal and regulatory approaches to help drive patient safety gains from HIE as well as avoid unintended patient safety risks.

4. Claudia Williams et al., *From the Office of the National Coordinator: The Strategy for Advancing the Exchange of Health Information*, 31 HEALTH AFF. 527, 533 (2012).

5. Peter C. Smith et al., *Missing Clinical Information During Primary Care Visits*, 293 JAMA 565, 568, 571 (2005).

6. Don Rucker, *Achieving the Interoperability Promise of 21st Century Cures*, HEALTH AFF. BLOG (June 19, 2018), https://www.healthaffairs.org/do/10.1377/hblog20180618.138568/full/.

7. Thomas Bodenheimer, *Coordinating Care—A Perilous Journey Through the Health Care System*, 358 NEW ENG. J. MED. 1064, 1070 (2008).

8. *See generally* Robert S. Rudin et al., *Usage and Effect of Health Information Exchange: A Systematic Review*, 161 ANNALS INTERNAL MED. 803 (2014).

9. Chaim M. Bell et al., *Association of Communication Between Hospital-Based Physicians and Primary Care Providers with Patient Outcomes*, 24 J. GEN. MED. 381, 382 (2009).

III. Efforts to Advance Interoperable Health Information Exchange

There has been substantial funding and activity at federal, state, and local levels to promote HIE in the United States.[10] However, the United States has not followed a single national approach to HIE. Instead, different approaches to HIE have emerged in healthcare markets based on community preferences for how to structure HIE in terms of the types of organizations involved (e.g., hospitals, ambulatory practices, and labs), the types of information that can be accessed (e.g., test results), and the form of electronic access (e.g., push and pull). Nonetheless, a common set of terms and definitions to describe key differences between market-driven approaches to HIE have emerged based on the types of "lead" organizations: Community HIE Networks, Enterprise HIE Networks, and EHR Vendor HIE Networks.[11]

Community HIE Networks—also referred to as Health Information Organizations (HIOs) or Regional Health Information Organizations (RHIOs)—exist when provider organizations in a given community collaborate to build the technical infrastructure and negotiate the governance approach to engage in HIE to improve patient care.[12] Typically, the only restriction on the types of stakeholders that can participate is geography. A recent survey found 119 of these networks in the U.S., and these networks are operating in 67% of healthcare delivery markets.[13] Hospitals and ambulatory providers were the most common types of participants in these networks, typically sharing test results and summary of care records across their EHR systems.[14]

Enterprise HIE Networks exist when one or more provider organizations electronically share clinical information to support patient care with some restriction, beyond geography, that dictates which organizations are involved. In contrast to Community HIE Networks,

10. *See, e.g.*, Williams et al., *supra* note 4, at 527 (discussing federal funding); Nat'l Opinion Research Center, *Evaluation of the State HIE Cooperative Agreement Program*, HealthIT.gov (Mar. 2016), https://www.healthit.gov/sites/default/files/reports/finalsummativereportmarch_2016.pdf (discussing state funding); Joshua R. Vest & Bita A. Kash, *Differing Strategies to Meet Information-Sharing Needs: Publicly Supported Community Health Information Exchanges Versus Health Systems' Enterprise Health Information Exchanges*, 94 Milbank Q. 77, 79 (2016) (discussing local funding).

11. Jordan Everson, *The Implications and Impact of 3 Approaches to Health Information Exchange: Community, Enterprise, and Vendor-Mediated Health Information Exchange*, 1 Learning Health Sys. 1, 1–3 (2017).

12. *Id.* at 1–2.

13. Julia Adler-Milstein, *Operational Health Information Exchanges Show Substantial Growth, but Long-Term Funding Remains a Concern*, 32 Health Aff. 1486, 1488–89 (2013).

14. *Id.* at 1488.

participation restrictions are driven by strategic, proprietary interests.[15] Although broad-based information access across settings would be in the best interest of the patient, provider organizations are sensitive to the competitive implications of sharing data and may pursue HIE in a strategic way.[16] A common scenario arises when hospitals choose to affiliate with select ambulatory providers, and invest in HIE capabilities with them, in order to encourage referrals from these providers to the hospital rather than to one of the competing hospitals.[17]

EHR Vendor HIE Networks exist when HIE occurs within a community of provider organizations that use an EHR from the same vendor. A subset of EHR vendors has made this capability available; Epic's CareEverywhere solution is the best-known example.[18] Providers with an Epic EHR are able to query for and retrieve key clinical data from any provider organization with Epic EHR that has activated this functionality. Little is known about the number of existing enterprise and EHR vendor HIE networks, the number of providers who use them, or the specific types of clinical information that are shared.[19] A small number of multi-vendor networks (e.g., CommonWell) have also emerged, in which a set of EHR vendors have developed the infrastructure and governance to allow data to be shared across the providers who choose to participate.

Increasingly, there are efforts to connect these varied networks to each other, such that a provider organization would only need to connect to one network in order to access all other networks. The final regulations for the so-called Trusted Exchange Framework and Common Agreement are expected from the United States Department of Health and Human Services Office of the National Coordinator (ONC) for Health IT in late 2018.[20] While participation will be volun-

15. Joshua R. Vest, *More Than Just a Question of Technology: Factors Related to Hospitals' Adoption and Implementation of Health Information Exchange*, 79 INT'L J. MED. INFORMATICS 797, 797–806 (2010).

16. *See generally* Joy M. Grossman et al., *Creating Sustainable Local Health Information Exchanges: Can Barriers to Stakeholder Participation be Overcome?*, CTR. FOR STUDYING HEALTH SYS. CHANGE, Feb. 2008, https://www.nihcm.org/pdf/Research_Brief_No._2_FINAL.pdf.

17. Joy M. Grossman & Genna Cohen, *Despite Regulatory Changes, Hospitals Cautious in Helping Physicians Purchase Electronic Medical Records*, CTR. FOR STUDYING HEALTH SYS. CHANGE, Sep. 2008, at 2–3, https://www.issuelab.org/resources/8986/8986.pdf.

18. T.J. Winden et al., *Care Everywhere, a Point-to-Point HIE Tool*, 5 APPLIED CLINICAL INFORMATICS 388, 389–90, 393–94 (2014).

19. Everson, *supra* note 11, at 5.

20. Office of the Nat'l Coordinator for Health Info. Tech., *Trusted Exchange Framework and Common Agreement*, HEALTHIT.GOV, https://www.healthit.gov/topic/interoperability/trusted-exchange-framework-and-common-agreement (last updated Feb. 28, 2018).

tary, to the extent that the approach is embraced by the market, it would vastly reduce the fragmentation of the varied networks that currently exist. Reducing fragmentation would increase the likelihood that a patient's data can be accessed regardless of where they receive care.

IV. Patient Safety Risks from HIE

While there are important differences between the approaches to HIE, regardless of approach, a set of corresponding human-mediated processes must be developed and consistently applied in order to translate HIE capabilities into safer and more effective care. When undertaking these processes, weaknesses in provider organizations' internal processes and standards are often exposed, which creates opportunities for errors and unsafe care. Two common types of errors, with implications for patient safety, can result when provider organizations pursue one or more approaches to HIE. The first type of error is related to patient identification and matching. The second type of error is related to efforts to protect patient privacy.

V. Risk 1: Errors Related to Patient Identification and Matching

Because the United States lacks a common individual identifier that can be used to match patient identity across provider organizations,[21] a key challenge facing any HIE effort is how to enable such identification and matching. This issue is particularly salient because of the potential patient safety implications that could emerge from incorrect identification and matching. Provider organizations typically have developed a set of policies and procedures that dictate patient identification and matching, such as how hospitals name newborn babies and unconscious, unidentified patients. When a provider organization chooses to share patient information electronically with other provider organizations, the naming principles are incorporated into the interface development between the two organizations' clinical information systems. Interfaces allow information to be delivered electronically and securely between separate clinical information systems, such as EHRs and laboratory information systems, which may not be using

21. Office of the Nat'l Coordinator for Health Info. Tech., HHSP233201300029C, Patient Identification and Matching Final Report 2–4 (Feb. 7, 2014), http://www.healthit.gov/sites/default/files/patient_identification_matching_final_report.pdf; *see generally* Michael D. Greenberg & M. Susan Ridgely, *Patient Identifiers and the National Health Information Network: Debunking a False Front in the Privacy Wars*, 4 J. Health & Biomedical L. 31 (2008).

the same vendor. Even if the two systems are from the same vendor, the organizations that wish to engage in HIE may not be using the same or compatible versions of the software. Patient matching and identification are critical to the development of an interface as they determine how information is sent and received electronically.

Patient identification and matching are particularly challenging in the case of the HIO approach to HIE because HIOs typically facilitate exchange across many provider organizations with many different vendor products and naming principles. Further, there is no standard set of attributes used for patient matching across organizations and not all attributes that an HIO may select for patient matching are collected in all EHRs.[22] Even patient medical record numbers do not offer a robust solution because, within a given provider organization, patients often have more than one number. This is due to the multiple patient and information management systems in use that are not interfaced with each other.

The role of the HIO (or other HIE approach) is to accommodate the multiple naming conventions used across provider organizations by managing the patient identity and matching process for incoming electronic clinical information. By maintaining a master patient index, the HIO can uniquely identify each patient so that clinical information can be shared across provider organizations. The HIO can accomplish this in a manner that supports successful patient identification and matching at each receiving provider organization. However, when patient identity and matching policies are not applied consistently at the provider organization, the logic built in to the interface with the HIO fails to work and the HIO may incorporate a temporary name as a real patient in their master patient index. For example, a given hospital's naming convention may be to use a gender identifier (i.e., female and male) as the first name and a rotating list of colors as the last name. If an unconscious male patient arrives at the hospital, and he is incorrectly entered into a hospital's EHR as "Man Brown" instead of "Male Brown," the interface would fail to identify "Man Brown" as a temporary name and a new person would be added to the HIO's master patient index as "Man Brown" when the hospital shares the clinical documents associated with this admission with the HIO. Clinical information associated with "Man Brown" could then be electronically sent to other provider organizations identified as one of the patient's providers, further propagating this failure in the patient identification and matching process and potentially creating false patients

22. PATIENT IDENTIFICATION AND MATCHING FINAL REPORT, *supra* note 21, at 12–13, 18, 27.

in multiple electronic record systems. Many provider organizations require active consent by their clinical or administrative staff to create new patient records when receiving electronic health information from an outside organization through an interface because of this issue. As a result, clinical information necessary for patients to receive safe and effective care may be incorrectly attributed to a false name or rejected by the receiving electronic record system because of intervention by clinical or administrative staff.

In addition, if another unconscious male patient is admitted at a later date and the same failure to follow the naming convention occurs at the same point in the color rotation, the records for the most recent patient could be combined with the records of the previous "Man Brown" patient. Once an incorrect match is made and records are merged, it is difficult to go back and appropriately assign each piece of clinical information to the correct patient. Rather than risk propagating incorrect information, the HIO will likely make all the information inaccessible to provider organizations, either by tagging the clinical documents so they are not viewable or by completely deleting them.

Thus, robust patient identification processes heavily depend on the actions of staff within provider organizations. Since these positions often have relatively high turnover rates, this creates a challenge for provider organizations to consistently apply carefully crafted policies and procedures.[23] Data quality issues that commonly exist within provider organizations include: spelling errors; incomplete patient identifiers; transposition of numbers and letters; and inconsistencies in conventions (such as how to handle hyphenated last names). In the case of HIE when this identifying information is shared, data quality issues propagate through the HIO's provider network and increasing the risk of failed or misidentification, both of which pose a risk to patient safety.

Patient matching—the process of ensuring recently created or received health information is added to the correctly identified patient's record—requires constant management within a provider organization and HIO. There is a fine balance between how patient matches are managed. If too stringent, the result is patients having multiple records and providers potentially missing critical information because they fail to find each of the records. If too flexible, patient records may get inappropriately combined resulting in inaccurate clinical information contained in the patient record.

23. *Id.* at 9.

VI. Legal & Policy Approaches to Reduce Errors Related to Patient Identification & Matching

To ensure effective patient identification and matching, multiple and broad infrastructure changes are critical. The ONC commissioned a project to evaluate current efforts to improve patient identification and matching as well as to provide recommendations for future efforts. The draft recommendations were reviewed by more than 150 organizations including health systems, HIE organizations, EHR vendors, and vendors of HIE solutions.[24] The final report, released in February 2014, provides recommendations that require action at multiple levels: from federal policy to EHR vendors, HIE organizations, and health care providers. The recommendations include infrastructure improvements, such as standardizing patient identifying attributes and including these attributes when information is electronically exchanged between provider institutions. Increasing and standardizing patient identification attributes would first require enhancements to EHRs. Therefore, the report recommends expanding the list of federally-certified attributes currently required in EHRs including a previous last name, middle name, as well as home, business, and cell phone numbers.[25] These newly-required elements would facilitate efforts to improve matching efficiency and accuracy, but are not commonly present.[26] There is ongoing work to implement this as well as to improve the accuracy of patient matching algorithms applied to the attribute data.

VII. Risk 2: Errors Related to Patient Privacy Protection

HIOs and other HIE approaches prioritize patient privacy protections to comply with state and federal law as well as to meet the expectations of provider organizations that have entrusted HIOs with the protected health information of their patients. Both provider organizations and patients must feel confident that there is an approach in place that will safeguard patient privacy. If provider organizations doubt the HIO's ability to protect patients' privacy, they will not share clinical information through the HIO. If patients doubt the HIO's ability to protect their privacy, they will actively prohibit their information from being shared with the HIO. As a result, HIOs invest in: (1) specific and detailed Data Use Agreements (DUAs) with their provider organization participants; (2) policies and procedures for the

24. *Id.* at 3.
25. *Id.* at 18.
26. *Id.*

maintenance and use of protected health information; and (3) privacy and security officers to monitor usage, conduct audits of access, and guide response to privacy and security inquiries by patients and provider institutions.[27]

Patient privacy is regulated by state and by federal law. States may have privacy laws that are more stringent than federal laws, particularly with regard to mental health. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides a foundation for privacy and security protections of health information in the United States. HIPAA regulates the electronic sharing of protected health information.[28] Protected health information includes clinical information that would identify a person and relay information about treatment for a medical condition or payment for health care services.[29]

Patient consent procedures determine whether patient information is accessible to providers participating in an HIO. As background, HIPAA requires patient consent when a provider queries for or requests information about a patient that resulted from care that the patient received from another provider (i.e., if a provider orders a diagnostic test, the ordering provider is not required to seek patient consent in order to receive the results of the diagnostic test. The patient's consent is assumed, given that she complied with the provider's order to have the test.). For example, a patient arrives indicating she was at an urgent care center or emergency department two nights ago and was told to follow-up with her primary care provider. In order to provide effective follow-up care, the primary care provider must be able to access the records of these results. However, to access the information from the urgent care center or emergency department, the patient's consent is required by HIPAA (whether access is obtained for paper records or electronic access).

To further complicate the picture, state-level patient privacy laws and associated consent requirements vary. In the context of HIE,

---

27. Genevieve Morris, *Trusted Exchange Framework and Common Agreement: A Common Sense Approach to Achieving Health Information Interoperability*, HEALTH IT BUZZ BLOG (Jan. 5, 2018), https://www.healthit.gov/buzz-blog/interoperability/trusted-exchange-framework-common-agreement-common-sense-approach-achieving-health-information-interoperability (discussing HIO business practices that motivated the drafting of the Trusted Exchange Framework and Common Agreement (TEFCA)).

28. *Summary of the HIPAA Privacy Rule*, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html (last visited Nov. 6, 2014).

29. OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., GUIDE TO PRIVACY AND SECURITY OF HEALTH INFORMATION 29, 32 (Apr. 2015), https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

there are two primary models of patient consent: opt-out and opt-in. The opt-out model assumes inclusion of all patients and their associated health information in the HIO unless patients opt-out from allowing the HIO to share their information across provider organizations in support of their care. Opt-in requires advance consent from patients to allow their information to be shared. In practice, there are many differences in how each model has been implemented. For example, one hybrid approach to patient consent is to treat patient information for physical health as opt-out while behavioral health information requires a patient to opt-in to allow this information to be shared with other providers. Behavioral health data has additional protections beyond HIPAA and state laws may be more restrictive than HIPAA.[30] Another protection for behavioral health data includes 42 C.F.R. § 2, which requires federally-funded substance abuse treatment centers to obtain patient consent to disclose patient identifiable information.[31] This hybrid consent model requires an HIE infrastructure that is capable of managing a sophisticated set of rules that addresses all possible combinations of data type (e.g., mental health, substance abuse, or physical health) and level of consent (e.g., yes to any provider, yes to specific providers, yes only in emergency care scenarios) that is not routinely available within HIOs. Many HIOs are limited by their technology to an all-or-nothing strategy in which all information on a patient is available or none is available. As a result, the majority of HIOs work with participating provider organizations to filter out behavioral health data from what is shared. A provider accessing patient information via the HIO would not know whether an absence of this information means the patient does not have any behavioral health conditions or whether the patient has these conditions but these conditions (as well as any associated medications, clinical notes, care plans, etc.) are not shared. This can lead to patient safety challenges when a patient's behavioral health information influences the safest and most effective course of treatment for physical health concerns.

VIII. Policy Solutions to Reduce Errors Related to Patient Privacy Protection

Current mechanisms are limited for achieving the dual goals of protecting patient privacy and pursuing safe and effective HIE. In partic-

30. *Behavioral Health Data Exchange Consortium ONC State Health Policy Consortium Project Final Report*, RTI Int'l (June 2014), https://www.healthit.gov/sites/default/files/bhdeconsortiumfinalreport_06182014_508_compliant.pdf [hereinafter RTI Int'l].

31. 42 C.F.R. § 2.13 (2017).

ular, there is a need to update regulations to accommodate new technologies while continuing to protect patient privacy. A key first step is harmonizing patient consent requirements under federal and state law. Some states have taken steps individually to modulate their privacy laws' stringency in order to facilitate HIE. For example, Hawaii, Kansas, Wisconsin, and Utah have passed legislation to allow HIE in accordance with HIPAA, eliminating more restrictive state requirements.[32] However, widespread harmonization remains elusive and a recent review of state laws relating to HIE concluded that much work remains to be done. As of 2016, among thirty-one states with laws addressing privacy and HIE, sixteen followed the opt-out approach, eight described an opt-in process, and the rest adopted other approaches to HIE participation. Twenty-three imposed specific confidentiality requirements on HIE users and five mentioned confidentiality without providing specific requirements.[33]

As an alternative to legal harmonization, mandated technical solutions could be pursued. With respect to particular types of sensitive data, there are ways to explore how technology can facilitate an approach to electronic exchange of sensitive data that also protects patient privacy. The ONC funded a Behavioral Health Data Exchange Consortium to identify and address challenges to exchanging behavioral health information.[34] The consortium made a number of recommendations. It determined that, to comply with more stringent consent requirements for sharing mental health and substance abuse information, the most expeditious route to enabling behavioral health HIE is to center these efforts on directed communications between providers.[35] While this strategy constrains the HIE approach to one-to-one communications between providers and does not enable query-based access to a community-wide health record, it does represent a means for sharing patient-specific behavioral health care information.

In addition, from 2013 through 2015 the ONC supported the development of a technical standard called Data Segmentation for Privacy

32. Kate Johnson et al., *Getting the Right Information to the Right Health Care Providers at the Right Time: A Road Map for States to Improve Health Information Flow Between Providers*, NAT'L GOVERNORS ASS'N 25 (Dec. 8, 2016), https://www.nga.org/center/publications/getting-the-right-information-to-the-right-health-care-providers-at-the-right-time-a-road-map-for-states-to-improve-health-information-flow-between-providers/.

33. Cason D. Schmit et al., *Falling Short: How State Laws Can Address Health Information Exchange Barriers and Enablers*, 25 J. AM. MED. INFORMATICS ASS'N 635, 638 (2018).

34. RTI INT'L, *supra* note 30.

35. *Id.*

(DS4P).[36] DS4P is a standard for adding a metadata tag to an electronic document to flag it as needing patient consent before being disclosed.[37] Historically, it has been difficult or impossible for providers to separate out parts of a patient's record that are subject to special consent requirements from parts that are not. The DS4P tag can help address this problem. However, this may not be a comprehensive solution and it is unclear whether DS4P is ready to be implemented at scale. Further, as long as DS4P remains an optional feature of certified EHR technology, providers will have to request—and pay extra for—the capability that DS4P offers. Even if they are willing to incur the cost, the practical value of DS4P could still be limited if provider organizations implement DS4P in non-standardized ways (i.e., by using an inconsistent set of rules for when and how to apply the tags).

Conclusion

Electronic Health Information Exchange is essential to ensure that, at both individual and population levels, providers and administrators have the information they need to make safe, effective, and efficient care decisions. As efforts at various levels of scale are pursued to ensure that HIE becomes ubiquitous, there are also important patient safety challenges that require attention. Specific provider organization practices, technology solutions, and policy efforts are needed to mitigate these specific patient safety risks from HIE.

36. Office of the Nat'l Coordinator for Health Info. Tech., *2015 Edition Final Rule: Data Segmentation for Privacy (DS4P)*, HealthIT.gov, https://www.healthit.gov/sites/default/files/2015editionehrcertificationcriteriads4p10615.pdf (last visited Oct. 26, 2018).

37. *Id.*