University of Colorado Law Review

Volume 90 | Issue 4 Article 5

Fall 2019

Medical Records and Privacy Rights: The Unintended Consequences of Aggregated Data in Electronic Health Records

Andrea C. Maciejewski

MEDICAL RECORDS AND PRIVACY RIGHTS: THE UNINTENDED CONSEQUENCES OF AGGREGATED DATA IN ELECTRONIC HEALTH RECORDS

Andrea C. Maciejewski*

In an era of rapid-pace technological innovation and political focus on healthcare, the federal government is pushing for nationwide interoperability of electronic health records. While there are many benefits from such a program, the lack of federal or state privacy regulations for patients' personal data opens up the possibility of widespread dissemination of private and sensitive information. This inattention to privacy will cause major problems if exploited.

Currently, there are no federal or Colorado laws that protect against potential privacy violations and provide recourse for a patient if a medical professional decides to insert non-medical information, such as information about the patient's housing status, into a patient's electronic health record without the patient's prior consent. Although innocuous enough when only the doctor has access to this record, with the increased use of health information exchanges, this information can be disseminated to thousands of healthcare providers around the country. This Comment argues that a comprehensive privacy protection act is critical and long past

---

* J.D. Candidate, 2019, University of Colorado Law School; Resource Editor, *University of Colorado Law Review*. Thank you to the many people who supported this project. In particular, I would like to thank Professor John Francis, Professor Margot Kaminski, and Professor Scott Skinner-Thompson for patiently working through different problems with me, diving into new and unknown territory, and providing thoughtful feedback; and my editors Vincent Forcinito, Joey DeAngelis, Shelby Krantz, and Hannah Regan-Smith for constantly pushing me to make this Comment better. I would also like to thank my mom for being a brilliant sounding board and wealth of knowledge, your insight and experience definitely helped me develop this Comment. And to Rand, thank you for your boundless support and patience throughout the many late nights and revisions, I could not have done this without you.

due for patient protection in the quickly evolving intersection of health care and technology.

INTRODUCTION 1112
I. AN OVERVIEW OF MEDICAL DATA DISSEMINATION, BIAS, AND CHOICE 1117
A. *The Legislative Push to Digitize and Aggregate Medical Records* 1118
B. *The Social Determinants of Health and Their Impact on Healthcare* 1120
II. CURRENT UNITED STATES MEDICAL RECORD LEGISLATION 1126
III. PRIVACY PROTECTIONS FOR SDH INFORMATION 1129
A. *Privacy Act of 1974—Direct Distribution of SDH Information by Agencies* 1131
B. *Federal Laws Controlling Distribution of SDH Information Through Public Records and Private Agreements* 1134
C. *State Laws Protecting Distribution of SDH Information* 1137
IV. SOLUTION 1143
A. *Overarching Federal Privacy Regulations* 1144
B. *Sector-Specific Federal Privacy Regulations* 1149
C. *Suggestions for State Regulatory Reform* 1152
D. *A Band-Aid Fix* 1154
CONCLUSION 1155

INTRODUCTION

Ten years ago, if a patient provided her personal information to a medical provider, there was a good chance that information was handwritten on a sheet of paper and stored in a folder in either the back of the provider's office or an offsite mass-storage facility.[1] The provider would have access only to

1. Fred Pennic, *80 Mind Blowing EMR and Meaningful Use Statistics and Trends*, HIT CONSULTANT (Oct. 30, 2012), https://hitconsultant.net/2012/10/30/80-mind-blowing-emr-and-meaningful-use-statistics-trends/ [https://perma.cc/X2YJ-PUZA] ("In 2011, 55% of physicians had adopted an electronic health record (EHR) system."); *EHR Adoption Rates—20 Must-See Stats*, PRACTICE FUSION (Mar. 1, 2017), https://www.practicefusion.com/blog/ehr-adoption-rates/ [https://perma.cc/9BHR-ZGE2] (statistic as of 2015) [hereinafter *EHR Adoption Rates*]; Eric Whitney, *Why Your Doctor May Still Have Paper Records*, KAISER HEALTH

the information the patient told him, and if the provider put something incorrect in the record, another provider or office might never see the flawed information.[2] Because medical records were kept as physical copies, patients had more control over who processed their health information and how the data was used.[3] Now, as electronic health records (EHR)[4] and other personal data become easy to access, a medical provider can almost instantly access a patient's comprehensive medical record that includes information that may or may not be relevant to the current procedure or need.[5]

This instantaneous access to a patient's EHR is compounded when the patient's provider is part of a health information exchange (HIE): a private company that networks with multiple healthcare providers to provide a common software that fluidly transmits patient EHR between providers.[6] Now,

---

NEWS (July 15, 2013), https://khn.org/news/colorado-doctors-and-big-leap-to-electonic-health-records/ [https://perma.cc/53KF-775M].

2. *Benefits of Modern EMR vs. Paper Medical Records*, PHOTO-STAT (June 17, 2015), https://photostat.org/benefits-of-modern-emr-vs-paper-medical-records/ [https://perma.cc/M6F8-PNZK]. When another provider needed a medical record, the paper record was often requested, sent to the primary provider, and then passed on to the patient who could give it to the next doctor. If a patient did not want to give the new doctor a paper record, this was their choice. EHR now make this information almost instantly accessible with less effort by the patient. An important contribution to information accuracy is the increased accuracy due to electronic typeface rather than often illegible medical provider's handwriting. Joseph Conn, *EHRs vs. Paper: A Split Decision on Accuracy*, MODERN HEALTHCARE (July 8, 2016), http://www.modernhealthcare.com/article/20160708/NEWS/160709938 [https://perma.cc/N3RC-324T].

3. This is referring to care given by different general practitioners or family practice doctors, not care for complex illnesses that have requirements for full medical records. Corinne Carey, *Are Patients About to Lose Control Over Their Medical Information?*, ACLU (June 6, 2012, 8:30 AM), https://www.aclu.org/blog/privacy-technology/are-patients-about-lose-control-over-their-medical-information [https://perma.cc/B3MG-2LLN].

4. An electronic health record is any electronically transmitted health record that includes patient demographics and medical health information and is used to aid the medical treatment of an individual. *Electronic Health Records*, CMS.GOV, https://www.cms.gov/Medicare/E-Health/EHealthRecords/index.html (last modified Mar. 26, 2012) [https://perma.cc/4NJH-CTRZ].

5. Carey, *supra* note 3 ("For example, does a foot doctor need to see a patient's records showing that she was a rape victim, had an abortion, underwent counseling, and took anti-depressants?").

6. One example is CORHIO, the Colorado-based HIE whose network is located almost exclusively in Colorado. *See Participating Providers*, CORHIO, http://www.corhio.org/participating-providers (last visited Mar. 4, 2018) [https://perma.cc/4NDY-3JU3]. As HIEs solidify their business models and become more profitable, more mergers occur amongst HIEs, which create larger networks. For an example, see Kate Monica, *Two CA Networks to Form Largest Health*

instead of a single provider having access to the patient's EHR, any doctor whom a patient visits within the HIE can automatically access the patient's EHR.[7] This is quite different than the days of paper records when a provider's access was limited to the specific information a patient chose to give him.

This data flow can become particularly problematic when social determinants of health (SDH) find their way into medical records. SDH are facts about a patient's social status that, while not necessarily critical for the actual provision of medicine, can help a healthcare provider craft a course of treatment tailored to a patient's health and lifestyle needs.[8] Whether through government and organizational databases or simply through public knowledge and records, medical providers are increasingly more likely to see nonmedical information, such as past incarceration information or housing status, when looking at a patient's EHR.[9] Within this new health information regime, instead of each patient maintaining the choice of who should have what information, aggregated SDH data paired with HIEs puts that choice into the hands of the provider.

Although this expansive access to personal information creates several privacy concerns, the advent of new technology combined with an understanding of how the medical profession can utilize SDH information to a patient's benefit is invaluable

---

Information Exchange, HIT INFRASTRUCTURE (Jan. 11, 2017), https://hitinfrastructure.com/news/two-ca-networks-to-form-largest-health-information-exchange [https://perma.cc/3QAS-QJZT]; *see also* Tom Sullivan, *What's Next for Health Information Exchanges?*, HEALTHCARE IT NEWS (Aug. 29, 2017), http://www.healthcareitnews.com/news/whats-next-health-information-exchanges [https://perma.cc/BPH8-G43C].

7. 45 C.F.R. § 164.506 (2018) does require prior patient authorization before sharing most medical EHR information with other providers who do not already have a relationship with the patient. However, HIEs provide an important loophole to this rule. HIEs have a choice of what type of consent policy they wish to choose. The Colorado HIE, CORHIO, uses an opt-out model where the default is that health information is available to any provider within the HIE without express patient consent. The opt-in model is friendlier toward patient privacy because it requires patient consent for each new provider who wishes to access the patient's EHR. MELISSA M. GOLDSTEIN & ALISON L. REIN, CONSUMER CONSENT OPTIONS FOR ELECTRONIC HEALTH INFORMATION EXCHANGE: POLICY CONSIDERATIONS AND ANALYSIS 5–7 (2010); OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., DRAFT TRUSTED EXCHANGE FRAMEWORK 18 (2018).

8. Rachel Gold et al., *Developing Electronic Health Records (EHR) Strategies Related to Health Center Patients' Social Determinants of Health*, 30 J. AM. BOARD FAM. MED. 428, 428–47 (2017), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5618800/ [https://perma.cc/JV9V-HAUH].

9. *See infra* Part I.

to providing higher quality care in a more efficient and cost-effective manner.[10] HIEs can reduce both the likelihood of redundant procedures and overall healthcare costs.[11] Doctors who understand a patient's personal life and history may be able to better adapt treatments and follow-up appointments to the patient's lifestyle and socioeconomic circumstances.[12] But the extensive visibility of private and potentially embarrassing information to healthcare providers, such as being homeless or having a record of felony convictions, can also lead to negative effects such as doctor bias and reduced quality of care.[13] Thus, as new technologies evolve and become more integrated and powerful, it is essential to balance the benefits to patients and society with the risks to individual privacy, and to address those risks early on.

This Comment explores the privacy issues associated with HIEs retrieving SDH information from outside sources for use within a patient's EHR.[14] Can an HIE legally obtain SDH

---

10. BD. ON POPULATION HEALTH AND PUB. HEALTH PRACTICE, INST. OF MED., CAPTURING SOCIAL AND BEHAVIORAL DOMAINS AND MEASURES IN ELECTRONIC HEALTH RECORDS: PHASE 2, at 43 (National Academies Press ed., 2014) ("To provide better patient care, improve population health, and enable more informative research, standardized measures of key social and behavioral determinants need to be recorded in electronic health records (EHR) . . . ."). The data collection of SDH in EHR is so new that the first empirical study to create effective tools of collection was published in 2017. Gold et al., *supra* note 8, at 1–2.

11. Jack Karsten, *Health Information Exchanges Reduce Redundant Medical Procedures*, BROOKINGS (May 26, 2017), https://www.brookings.edu/blog/techtank/2017/05/26/health-information-exchanges-reduce-redundant-medical-procedures/ [https://perma.cc/3AKF-XQ3M].

12. AUGUSTUS A. WHITE III ET AL., SEEING PATIENTS: UNCONSCIOUS BIAS IN HEALTH CARE 250 (Harvard Univ. Press ed., 2011). An acute example of these benefits is shown by a doctor's knowledge of incarceration data. In the criminal system, many mentally ill offenders are considered "frequent flyers." Due to the lack of coordination between the jail system and healthcare system, most inmates leaving the jail system receive little-to-no mental health aftercare. This leads to cases where individuals are arrested over and over again in short periods of time, leading to poor quality of life and trauma for an individual as well as huge burdens on local police and jails. E. FULLER TORREY ET AL., MORE MENTALLY ILL PERSONS ARE IN JAILS AND PRISONS THAN HOSPITALS: A SURVEY OF THE STATES 9 (Nat'l Sheriffs Ass'n & Treatment Advocacy Ctr., 2010) (including examples of a Palm Beach individual with schizoaffective disorder who was arrested forty-nine times over forty months, a Houston woman diagnosed with schizophrenic disorder who was charged with twelve felonies and thirty-one misdemeanors over the course of ten years, and a woman in Memphis who was finally committed to a state psychiatric hospital after 259 arrests).

13. *See infra* notes 52–54.

14. Although there are currently no reports or articles about HIEs retrieving SDH information with or without a patient's consent, this is likely because the

information from an outside source and subsequently insert it into the EHR? If they can distribute SDH information to the network without an individual's permission, should they? Once the information is placed into the EHR, can a patient offset the aggravating factor of mass dissemination? This Comment uses the privacy of a person's housing status to exemplify the lack of protections for SDH information. Other types of SDH information (e.g., incarceration records, access to food, sexual orientation, political affiliation, etc.) will not be addressed in this Comment but can be analyzed in a similar fashion.

Part I gives an overview of data aggregation through EHR and HIEs and briefly describes doctor bias in medical care. Part II examines current federal legislation focused on EHR and healthcare. Part III focuses on the current privacy protections afforded to an individual's SDH information by federal law and Colorado state laws. Finally, Part IV puts forth recommended solutions that better protect individuals by implementing data processing limitations and enabling private causes of action, which can provide patients more control over their SDH information when used in EHR.

Ultimately, the United States should move toward an overarching federal privacy protection policy for citizens mod-

---

topic is very new. Incentivized by recent legislation, HIEs are currently looking to the legality and feasibility of using SDH information in HIEs. A prime example can be seen through an email sent by a large HIE to the author:

> [Private HIE] is pursuing opportunities to expand from "healthcare" to "health" in its data acquisition strategy. We believe the key to the Triple Aim is ensuring that patients and their care providers have access to all meaningful data that impacts their health. We believe that the combination of traditional healthcare data with social determinants of health and genomics provides a powerful set of information to promote precision medicine and predictive analytics. [State Agency] is also promoting this evolving thinking.
>
> To most effectively pursue the integration of these additional data sources that are often not governed by HIPAA, [Private HIE] needs help in two main areas:
>
> 1. Legal. What are the legal implications of sharing social determinant and genomic data with healthcare providers (with and without patient consent)?
> 2. Policy Recommendations. As an example: just because we can share with a physician that her patient has been recently incarcerated, should we? Does this help or hurt the patient-provider relationship? The patient's trust of the system? The patient's ability to be self-empowered in his or her care?

E-mail from Chief Strategy Officer, Anonymous Private HIE (June 26, 2016, 9:59 AM) (on file with author) (edited for anonymity purposes).

eled on the current privacy laws of the European Union.[15] While a potential federal law is in the throes of a long democratic process, Colorado should protect its citizens by adopting state privacy standards similar to California's medical privacy laws and "Shine the Light" laws.[16] Although individual state action is not as effective as federal regulation, it is an adequate gap-filler until Congress is able to come to a consensus on just what information should be protected and how to protect and manage this information.

I. AN OVERVIEW OF MEDICAL DATA DISSEMINATION, BIAS, AND CHOICE

The United States is currently undergoing a healthcare revolution. Issues of access and quality in healthcare have led to dozens of new laws, regulations, and policy announcements in the past year alone.[17] The emphasis on the digitization of medical records and the federal government's push to utilize more social determinants of health (SDH) means that many in the healthcare industry are turning to electronic health records (EHR) as a means of collecting SDH.[18] And although the United States has attempted to protect the privacy of individuals' medical information, policy shifts in the utilization of SDH, expansion of EHR, and connection of EHR through health information exchanges (HIEs) raise privacy questions

15. *See infra* Part IV for the full solution analysis.

16. This Comment focuses mainly on Colorado law. It suggests that Colorado follow California's lead in privacy laws. *See infra* Part III; John W. McGuinness & Christina J. Weis, *Shine-the-Light Law: California's Latest Class-Action Trend*, ABA (Apr. 17, 2012), http://apps.americanbar.org/litigation/committees/consumer/email/spring2012/spring2012-0402-shine-light-law-californias-latest-class-action-trend.html [https://perma.cc/QG72-2MX4]; Michael R. Geroe & J. Keith Biancamano, *Shining the Light on California's "Shine the Light" Law*, ACC DOCKET, Sept. 2012, at 64, https://www.gibsondunn.com/wp-content/uploads/documents/publications/Biancamano-ShiningtheLight.pdf [https://perma.cc/T6LK-6SVS] (explaining that the "Shine the Light" law allows individuals to request information about what private information was shared and to whom from private entities that have access to their data and gives a private right of action for failures to provide information as well as information breaches).

17. *Federal Policy on Healthcare, 2017-2020*, BALLOTPEDIA, https://ballotpedia.org/Federal_policy_on_healthcare,_2017-2020 (last visited Mar. 4, 2017) [https://perma.cc/F4DB-8DNQ].

18. BD. ON POPULATION HEALTH AND PUB. HEALTH PRACTICE, *supra* note 10; INST. OF MED., CAPTURING SOCIAL AND BEHAVIORAL DOMAINS AND MEASURES IN ELECTRONIC HEALTH RECORDS: PHASE 2, at 43 (National Academies Press ed., 2014).

regarding who decides what information to process and in which scenarios.

A. *The Legislative Push to Digitize and Aggregate Medical Records*

Congress is putting an immense amount of money (over $36 billion) and political energy into expanding EHR.[19] EHR are electronic versions of a patient's medical history that include clinical data and other relevant information, as determined by the medical provider.[20] The government's influx of funding and attention is establishing EHR as the predominant way of maintaining patient information. Less than a decade ago, 90 percent of physicians were entering medical-record data into paper records by hand, whereas now over 87 percent of physicians are using an EHR system.[21]

As EHR become more useful and convenient, doctors are further aggregating their data by joining HIEs. HIEs are private companies that have a network of healthcare providers who all use a common software program to fluidly transmit patient EHR between providers.[22] This interoperability (the extent to which devices can exchange and interpret shared data) allows data aggregation and easier transmission of patient medical records between participating providers. Although HIE aggregation and transmission currently only affect private enterprises, Congress has stated that the "meaningful use of interoperable electronic health records throughout the United States . . . [is] a critical national goal."[23] Thus, between the 2009 Health Information Technology for Economical and Clinical Health Act (HITECH)[24] and the 2016 21st Century Cures

---

19. *Meaningful Use*, CDC.GOV, https://www.cdc.gov/ehrmeaningfuluse/introduction.html (last updated Jan. 18, 2017) [https://perma.cc/6DYX-NSC4]; *see* 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033 (codified at 42 U.S.C. §§ 300jj(11)–(14) (Supp. V 2018)); *EHR Adoption Rates*, *supra* note 1; Brian Shilling, *The Federal Government Has Put Billions into Promoting Electronic Health Record Use: How Is It Going?*, COMMONWEALTH FUND, http://www.commonwealthfund.org/publications/newsletters/quality-matters/2011/june-july-2011/in-focus (last visited Mar. 4, 2018) [https://perma.cc/Z9JK-ZGUG].

20. *Electronic Health Records*, *supra* note 4.

21. *EHR Adoption Rates*, *supra* note 1.

22. *See Participating Providers*, *supra* note 6.

23. *Meaningful Use*, *supra* note 19.

24. Pub. L. No. 111-5 § 13410(d)(3)(A–D) (2009) (codified at 42 U.S.C. § 17939 (2012)).

Act (Cures Act),[25] the United States has dedicated over $36 billion to creating a completely interoperational EHR system.[26]

The Cures Act, in particular, includes a pointed push toward nationwide interoperability of EHR.[27] By directing the Office of the National Coordinator for Health Information Technology to create a Trusted Exchange Framework where all HIEs can share patient data, Congress is effectively encouraging the creation of one nationwide HIE.[28] Within the Trusted Exchange Framework, "there is no limitation to the aggregation of data that is exchanged among [p]articipants."[29] A system of this size and breadth will enable doctors all over the country to access the complete record of any patient, regardless of where that patient last received care.[30]

EHR housed in HIEs can be both a blessing and a curse for patients. For example, when there is a reliable mechanism for sharing patient medical records, such as an HIE, patients who need treatment at different locations over time will be less likely to receive duplicate procedures and tests, thus reducing costs overall.[31] The increased transparency across HIEs also reduces the likelihood of a patient undergoing unnecessary pro-

---

25. Pub. L. No. 114-255, 130 Stat. 1039 (codified at 42 U.S.C. §§ 300jj-11–14 (Supp. V 2018)).

26. *Id.*; Robert O'Harrow Jr., *The Machinery Behind Health-Care Reform*, WASH. POST (May 16, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/05/15/AR2009051503667_2.html [https://perma.cc/7UQZ-Y6LG]; *cf.* Jonathon H. Roth, *Regulating Your Medical History Without Regulations: A Private Regulatory Framework to Electronic Health Record Adoption*, 91 B.U. L. REV. 2103, 2104 (2011) (claiming the amount is $27 billion, rather than $37 billion).

27. 42 U.S.C. § 300jj (Supp. V 2018); *id.* § 300jj-11.

28. *Id.* § 300jj-11; OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., *supra* note 7, at 7. This draft was put out for public comment. The Office of the National Coordinator for Health Information Technology published an easy to use guide to understanding the Draft Trusted Exchange Framework. OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., A USER'S GUIDE TO UNDERSTANDING THE DRAFT TRUSTED EXCHANGE FRAMEWORK, https://www.healthit.gov/sites/default/files/draft-guide.pdf (last visited Jan. 19, 2019) [https://perma.cc/8FX3-CYS4].

29. OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., *supra* note 28, at 11.

30. *Meaningful Use*, CENTER FOR DISEASE CONTROL AND PREVENTION (last updated Jan. 18, 2017), https://www.cdc.gov/ehrmeaningfuluse/introduction.html [https://perma.cc/8DCT-JHFD].

31. Jack Karsten, *Health Information Exchanges Reduce Redundant Medical Procedures*, BROOKINGS (May 26, 2017), https://www.brookings.edu/blog/techtank/2017/05/26/health-information-exchanges-reduce-redundant-medical-procedures/ [https://perma.cc/CN9U-R547].

cedures and the risks associated with those treatments.[32] Despite the benefits, there is a dark side to large HIE systems and data aggregation. These systems can be exploited to a patient's detriment by gathering and disseminating information only tangentially related to immediate medical care without patient knowledge or consent. This extraneous use risks processing data in ways that the patient never anticipated at the time the patient gave consent for the collection of that data. For example, a piece of information given to a patient's family doctor of twenty years can be processed by other providers in a participating HIE with which the patient may not have any history or experience. This loss of the data's contextual integrity is only compounded when EHR begins using SDH.[33]

B. The Social Determinants of Health and Their Impact on Healthcare

Simultaneously with the push for the digitization of medical records, policy efforts are increasingly focused on bringing SDH to the forefront of modern medical inquiry.[34] To reiterate, SDH are nonmedical facts about a patient—such as housing status, education, and religious beliefs—that can help a healthcare provider create more customized treatment plans that account for a patient's potentially extraordinary circumstances.[35] Alongside the benefits to individual patients, the use of SDH information in medical records may also allow the government to see trends in healthcare, which enables more informed research and ultimately better broad-reaching solutions.[36]

---

32. *Id.*

33. Contextual integrity refers to the privacy theory that information is given in a very specific context. The context in which it is given defines how the giver expects that information will be used and processed. *See* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 136–55 (2004). "For example, the norms of a parent-teacher conference dictate that a teacher can reveal information about the parent's child to the parent, but not about other children." Priya Kumar, *How the Contextual Integrity Framework Helps Explain Children's Understanding of Privacy and Security Online*, FREEDOM TO TINKER (Dec. 6, 2017), https://freedom-to-tinker.com/2017/12/06/how-the-contextual-integrity-framework-helps-explain-childrens-understanding-of-privacy-and-security-online/ [https://perma.cc/S64L-FQ8H].

34. BD. ON POPULATION HEALTH AND PUB. HEALTH PRACTICE, *supra* note 10, at 43.

35. Gold et al., *supra* note 8.

36. BD. ON POPULATION HEALTH AND PUB. HEALTH PRACTICE, *supra* note 10, at 1 ("To provide better patient care, improve population health, and enable more

Because of SDH's usefulness in showing overall trends, it makes sense that a number of government initiatives increasingly demand aggregated databases of SDH to improve the efficiency and effectiveness of government programs.[37] For example, the McKinney-Veto Act requires organizations that receive funding under the Act to "ensure operation of, and consistent participation by, project sponsors in a community-wide homeless management information system [HMIS]."[38] Participants enter extensive SDH information into the system with the aim of sharing data across organizations involved in the care of a homeless individual.[39] Aggregated data in an HMIS can include (but is not limited to) contact information, social security numbers, mental health information, substance abuse history, employment, and education.[40]

Although there are data and technical standards informing the HMIS, a "covered homeless organization" may disclose personally identifiable information from an HMIS "to provide or coordinate services to individuals."[41] Thus, as long as a department can articulate its guiding data-collection policy, which has the purpose of coordinating services for homeless individuals, HMIS records can migrate into a participating healthcare system.[42]

---

informative research, standardized measures of key social and behavioral determinants need to be recorded in electronic health records (EHR) . . . ."). The data collection of SDH in EHR is so new that the first empirical study to create effective tools of collection was published in 2017. Gold et al., *supra* note 8, at 1–2.

37. DANIEL SOLOVE, UNDERSTANDING PRIVACY 117–19 (2008).

38. 42 U.S.C. § 11360a(f)(3) (2012) (as amended by the Homeless Emergency Assistance and Rapid Transition to Housing Act of 2009).

39. *HMIS Requirements*, HUD EXCHANGE, https://www.hudexchange.info/programs/hmis/hmis-requirements/ (last visited Sept. 21, 2018) [https://perma.cc/G8NP-QNS6].

40. ABT ASSOCS., INC., HOMELESS MANAGEMENT INFORMATION SYSTEM DATA AND TECHNICAL STANDARDS NOTICE: FREQUENTLY ASKED QUESTIONS 3–4 (2005), https://www.in.gov/ihcda/files/hmis_data_standards_faq.pdf [https://perma.cc/F9F5-GUDR].

41. *Id.* at 24; Data and Technical Standards Final Notice, 69 Fed. Reg. 45,888–45,934 (July 30, 2004), https://www.hudexchange.info/resources/documents/2004HUDDataandTechnicalStandards.pdf [https://perma.cc/SUR7-8959].

42. The Human Services Agency of San Francisco published a guidance document on homeless coordination that explained: "So long as the new department articulates CE as its guiding data collection policy and adequately advises clients of this policy in its HMIS privacy notice, the HMIS *Data and Technical Standards* seems to allow for database integration and historical records migration under the 'coordinating services' allowance . . . ." PETER RADU, HUMAN SERVICES AGENCY, CITY AND COUNTY OF SAN FRANCISCO, EVERYTHING

Once the healthcare system has the HMIS information, the information can then trickle into a patient's EHR.[43] In fact, the Department of Housing and Urban Development (HUD) acknowledges that there are very few limits imposed by the Health Insurance Portability and Accountability Act (HIPAA), which enables the main federal regulation on the privacy and security of medical records,[44] on what a covered entity can and cannot collect from outside sources (including other participating agencies).[45] Although the flow of nonmedical data from an HMIS into an individual's EHR is cause for concern, the pros and cons of creating an HMIS are beyond the scope of this Comment.

The true problem occurs when the same health system that is part of the HMIS is also part of an HIE. Here, the information that was collected at a non-health-related participating agency—such as a job-training organization—and transferred to a participating healthcare system that placed all or some of that information into a patient's EHR, is now available to any healthcare system in the HIE. The scope of this problem will expand exponentially should the federal government achieve its vision of a national HIE. Imagine that an individual told her job-training counselor that she recently became homeless and needed help figuring out what address to put on employment applications. This disclosure is entirely dependent on the context of that specific situation, including the trust she has in the counselor and her needs at that time.[46] If the patient later went to a doctor's appointment at a health system that was part of the same HMIS as the job-training center, her provider could have information about her housing status, whether or not she was willing to give him that information at all.

THAT HOUSES MUST CONVERGE: COORDINATED ENTRY, HMIS, AND A CENTRALIZED DATABASE FOR A NEW DEPARTMENT 47 (Apr. 18, 2016) (on file with author).

43. *E.g.*, *id.*

44. 45 C.F.R. pt. 160 (2018).

45. ABT ASSOCS., INC., *supra* note 40, at 7 ("The only limitation on *collection* applies when a covered entity requests PHI *from another covered entity*. In that case, a requester must sometimes make reasonable efforts to limit the request to the minimum information necessary to accomplish the intended purpose of the request (45 C.F.R. § 164.502(b)(1)). This provision is not a general limitation on the collection of information and does not restrict data collection from a data subject.").

46. Nissenbaum, *supra* note 33.

As this Comment discusses, there are many benefits to a provider knowing SDH information, but the choice of whether providers have that information at all should lie with the patient, or at least with a privacy proxy that keeps the patient's best interest in mind.[47] This type of scenario motivates this Comment's emphasis on proactively closing the privacy loophole before it becomes a more serious problem.

Similar to the use of HIEs, a doctor's knowledge of SDH can increase quality of care and lower overall healthcare costs. Doctors who understand a patient's personal life and history may be able to adapt things like treatments, appointments, and prescription pickups to fit a patient's extenuating circumstances, such as a lack of transportation or lack of running water.[48] Despite the benefits, a provider's knowledge of certain SDH information can also have potential detrimental effects on the patient's care.

While most doctors have few negative reactions to low-income or homeless individuals, research suggests that the knowledge of certain SDH can lead to implicit doctor bias.[49] Implicit doctor bias includes both reduced access[50] and reduced empathy, both of which can lead to lower quality of care for patients in difficult life situations.[51] For example, from an access standpoint, low-income women are 25 percent less likely to be screened for breast cancer during an appointment than high-income women.[52] Although there are no studies directly connecting implicit bias to the quality of care given to homeless

47. *Infra* Part IV.

48. *See* WHITE III ET AL., *supra* note 12, at 250.

49. *See* Alison G. Fine et al., *Attitudes Towards Homeless People Among Emergency Department Teachers and Learners: A Cross-Sectional Study of Medical Students and Emergency Physicians*, BMC MED. ED., Aug. 23, 2013, at 1; *see also* Matthew J. To et al., *Homelessness in the Medical Curriculum: An Analysis of Case-Based Learning Content from One Canadian Medical School*, 28 TEACHING & LEARNING IN MED. 35 (2016) (looking at how homelessness is portrayed in one Canadian school's medical education).

50. Access is defined as a patient's ability to enter into the healthcare system, access a location where needed health services are provided, and find a provider who the patient trusts and can communicate with. *Access to Health Services*, HEALTHYPEOPLE.GOV, https://www.healthypeople.gov/2020/topics-objectives/topic/Access-to-Health-Services [https://perma.cc/V9UG-TJJB].

51. Robert Pearl, *Why Health Care Is Different if You're Black, Latino, or Poor*, FORBES (Mar. 5, 2015, 12:59 PM), https://www.forbes.com/sites/robertpearl/2015/03/05/healthcare-black-latino-poor/ [https://perma.cc/2XYR-2XBY].

52. *See* TORREY ET AL., *supra* note 12; WHITE III ET AL., *supra* note 12; Fine et al., *supra* note 49; To et al., *supra* note 49.

individuals, studies linking negative attitudes toward other at-risk groups with quality of care are illuminating.[53] For instance, prejudicial attitudes of physicians and therapists toward patients with mental health issues have direct consequences on the quality of care given to those patients.[54]

Even if a doctor does not let his implicit bias affect the procedures performed, that bias can manifest in his general attitude toward a patient. In a study exploring attitudes toward homeless individuals in the emergency room, between 5 and 10 percent of all professionals who participated in the study felt that homeless people choose to be homeless.[55] In one survey, only 69.7 percent of people believed that "[h]ealth care dollars should be directed toward serving the poor and homeless . . . ."[56] Significantly, 6.74 percent of all doctors in the survey stated that they "resent the amount of time it takes to see homeless patients."[57] Another recent study found that homelessness was often associated with stereotypes "such as individuals living with schizophrenia or exhibiting self-neglect and destructive personal behaviors," all of which could contribute to "[medical] students' less favorable attitudes toward vulnerable populations over time."[58] Negative attitudes toward homeless patients do not go unnoticed by patients. A study

---

53. *See* April Dembosky, *Training Doctors to Spot Their Own Biases*, CNN (Sept. 7, 2015, 9:04 AM), https://www.cnn.com/2015/09/07/health/healthcare-racial-bias/ [https://perma.cc/5S9R-K26B] ("[S]everal studies show that African-American patients are often prescribed less pain medication than white patients with the same complaints."); *see also* P. Mannava et al., *Attitudes and Behaviors of Maternal Health Care Providers in Interactions with Clients: A Systematic Review*, 11 GLOBALIZATION & HEALTH 36 (2015), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4537564/ [https://perma.cc/TN7B-XYCC]. The study by P. Mannava et al. used systematic methods to review peer-reviewed literature. Of the studies used, none were done in the United States. However, this Comment looks to this research for the effects of bias on quality of care in human nature. Additionally, the broad range of countries that were looked at should cancel out some, if not most, of the cultural biases that are potentially unrelated to American medicine.

54. *See generally* Stephanie Knaak et al., *Mental Illness-Related Stigma in Healthcare: Barriers to Access and Care and Evidence-Based Solutions*, 30 HEALTHCARE MGMT. F. 111 (2017).

55. Fine et al., *supra* note 49, at 3 tbl. 1.

56. *Id.* Medical students in their first or second year gave a positive response 69.7 percent of the time, medical students in their third or fourth year gave a positive response 68.8 percent of the time, and ER residents and staff gave a positive response only 62.7 percent of the time. *Id.*

57. *Id.*

58. To et al., *supra* note 49, at 39.

conducted in 2017 showed that 40 percent of homeless people reported being judged unfairly or treated with disrespect by a medical professional in the past year.[59]

It must be acknowledged that these biases are not present in every doctor, or perhaps even most doctors. As the data suggests, most doctors are good, caring medical professionals who provide the same quality of care regardless of a patient's income level or past life experience.[60] However, there is a chance that an individual's current status of homelessness or other nonmedical information might affect the quality of care she gets from her doctor. This risk should not be predetermined by the location of a patient's medical record—such as an EHR located in an HIE—or by the secondary use of information originally provided for a nonmedical function—such as job training—but should instead be the patient's choice. Every individual should be able to assess the doctor in front of her and decide whether she trusts this person with sensitive, private, and perhaps embarrassing information that could change the course of her medical care.

When a third party places information into an EHR without the explicit consent or knowledge of a patient, the patient has no choice about how her information is later disclosed and to whom. Even if the original processing of the data was understood and consented to by the patient, future unrelated use of that data deprives the patient of her choice about how her information is processed and prevents the information from maintaining its contextual integrity. Federal laws currently protect people's information from being disseminated to inappropriate third parties once that information is within the medical record, but is this our only concern?[61] What happens to data that was never intended to be shared with medical providers? Does a patient have a right to decide whether every doctor in the country should have access to information that she is homeless, an ex-convict, or a food stamp recipient? Should we require citizens to voluntarily give this information,

---

59. Aaron Sibley et al., *An Inner City Emergency Medicine Rotation Does Not Improve Attitudes Toward the Homeless Among Junior Medical Learners*, CUREUS, Oct. 5, 2017, at 1, 6.

60. While there is no source for this opinion, my argument presumes that this is true and focuses on the potential of the minority of doctors to misuse information.

61. *See infra* Part II (discussing HIPAA privacy protections).

or is it satisfactory that we simply protect the information once it enters their medical records?

Current privacy laws protect sensitive personal information once it is within the EHR, but there is nothing blocking sensitive data, including SDH, from being entered into the EHR in the first place.[62] As the United States moves toward more connected technology and robust government databases, the failure to address privacy issues associated with how we get information into the EHR will only make the negative consequences of HIEs more widespread and harder to contain. By analyzing the privacy implications of EHR in HIEs before the United States reaches a national HIE, lawmakers can create laws that address the unintended consequences of mass medical data aggregation and restrict medical providers' ability to access outside private information and place it in a patient's EHR without consent.

II. CURRENT UNITED STATES MEDICAL RECORD LEGISLATION

Understanding HIPAA regulations is essential to understanding how data is protected both as it enters a medical record and as it is disseminated to other healthcare providers.[63] EHR house an immense amount of personal information about patients' healthcare systems.[64] This information includes both basic medical data (treatment history, medications, vaccinations, etc.) as well as personal information (race, language, addresses, email addresses, social security numbers, etc.).[65] Both medical data and personal information are considered protected health information (PHI) if they are in a patient's EHR.[66] HIPAA's Privacy Rule explains how covered entities

62. Trisha Torrey, *Are Medical Records Private?*, VERYWELLHEALTH (Nov. 5, 2018), https://www.verywell.com/who-has-access-to-your-medical-records-2615502 [https://perma.cc/CMT9-QJT6]; *see also infra* Part II (discussing HIPAA laws that protect information once it is in the EHR).

63. *See generally* 45 C.F.R. pt. 160 (2018) (explaining the general requirements and purpose of HIPAA).

64. *See* 45 C.F.R. § 170.102 (2018) (An EHR is any record that "[h]as the capacity (i) [t]o provide clinical decision support; (ii) [t]o support physician order entry; (iii) [t]o capture and query information relevant to health care quality; (iv) [t]o exchange electronic health information with, and integrate such information from other sources.").

65. *Id.*

66. 45 C.F.R. § 170.102; *About Protected Health Information (PHI)*, IND. U., https://kb.iu.edu/d/ayyz (last updated Jan. 10, 2019) [https://perma.cc/YHS8-

may consolidate, use, and disclose PHI.[67] A covered entity that fails to use PHI appropriately is required to follow certain notification requirements and is also subject to civil and criminal penalties that can be as costly as $50,000 per individual violation.[68] There is no private right of action under HIPAA.[69] In the event of data misuse under HIPAA, private individuals can do little more than submit a complaint to the Office of Civil Rights (OCR). OCR may investigate and conduct a compliance review before sanctioning the entity, but this is at OCR's sole discretion.[70] Otherwise, an individual must turn to private tort action to recover for a breach of their private information.[71] States may also bring a privacy lawsuit on behalf of their citizens.[72]

EHR can be efficiently shared among healthcare providers through an HIE.[73] HIEs distribute EHR across different

---

L9UA]. PHI is defined as individually identifiable information transmitted or maintained by any medium. It is further broken down by identifying specific types of information that must be de-identified before information can be disclosed to third parties that are not covered entities as defined by HIPAA. Information that must be de-identified includes eighteen identifiers, such as names, telephone numbers, addresses, and email addresses. 45 C.F.R. § 160.103 (2018); *Id.* § 164.514.

67. *About Protected Health Information (PHI), supra* note 66. Covered entities are all entities that are subject to the regulations of HIPAA privacy standards. These include "(1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by [subchapter C of Title 45]." 45 C.F.R. § 160.103 (2018); 87 AM. JUR. 3D *Proof of Facts* § 259(I)(A)(§5) (2018).

68. 45 C.F.R. § 160.404(b) (2018); *see also HIPAA Information—Frequently Asked Questions*, GERONNURSING & RESPITE CARE, INC., http://www.geron nursinginc.com/HIPAA.html (last visited Mar. 12, 2018) [https://perma.cc/8TJL-YUJQ]. The original maximum civil penalty was $25,000 per violation, but the HITECH Act recently increased the amount to $50,000. Pub. L. No. 111-5 § 13410(d)(3)(A–D) (2009) (codified at 42 U.S.C. § 17939 (2012)).

69. Arcara v. Banks, 470 F.3d 569, 571 (5th Cir. 2006); Univ. of Colo. Hosp. v. Denver Pub. Co., 340 F. Supp. 2d 1142, 1145 (D. Colo. 2004) (holding that HIPAA does not contain a private right of action).

70. BUSINESS AND LEGAL RESOURCES, EMPLOYER'S GUIDE TO THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT ¶ 820 (2018), Westlaw 4171630.

71. *Id.*

72. *Id.*

73. There are three types of HIEs: directed exchange, query-based exchange, and consumer-mediated exchange. *What Is HIE?*, HEALTHIT.GOV, https:// www.healthit.gov/topic/health-it-and-health-information-exchange-basics/what-hie (last visited Mar. 18, 2018) [https://perma.cc/5ALA-S3F4]; *Health Information Exchange*, USFHEALTH ONLINE, https://www.usfhealthonline.com/resources/key-concepts/health-information-exchange-hie/ (last visited Jan. 18, 2019) [https:// perma.cc/9R7Q-F6DH]. This Comment focuses on directed exchanges and query-

healthcare practices within the respective network and enable PHI to be exchanged among entities participating in the network.[74] HIEs are subject to HIPAA privacy rules under the "business associate" definition.[75] A business associate is any person who maintains, creates, receives, or transmits PHI on behalf of a covered entity.[76] Thus, HIEs are subject to the same HIPAA rules and regulations that covered entities, such as providers and payors, must follow.[77] Once the HIE receives PHI from an individual, the HIE must protect that information or open itself up to liability for a breach of privacy.[78]

The data structure of an HIE allows extremely sensitive information to be passed along to hundreds of doctors within a network. Some of this sensitive information is voluntarily given, while some is deduced during medical exams or treatments. But what of the information that is assumed or retrieved from external databases and added without a patient's knowledge or consent? HIPAA gives a patient the right to access her records, and even a right to request a change to the medical record, but it does not require a doctor to actually change the information or remove it simply because someone does not want it on the record.[79] A doctor's ability to refuse a

---

based exchanges, which allow providers to send and receive PHI to and from other providers within the network.

74. OFFICE OF CIVIL RIGHTS, THE HIPAA PRIVACY RULE AND ELECTRONIC HEALTH INFORMATION EXCHANGE IN A NETWORKED ENVIRONMENT 2 (2009), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/introduction.pdf [https://perma.cc/TB28-Y7UE]. The most common types of HIEs are Regional Health Information Organizations.

75. 45 C.F.R. § 160.103 (2018); CORHIO, HIPAA AND HEALTH INFORMATION EXCHANGE, http://www.corhio.org/library/documents/PDF_Collateral/hipaa_and_hie.pdf (last visited Jan. 18, 2019) [https://perma.cc/M8F4-RHLU].

76. 45 C.F.R. § 160.103.

77. *Id.* § 160.404 (2018).

78. *Id.*; 42 U.S.C. § 1320d-6 (2012). HIPAA provides a tiered civil penalty structure and some criminal penalties for HIPAA violations. For an overview of the tier structure, see Kim Stanger, *Complying with HIPAA: A Checklist for Business Associates*, HOLLAND & HART (Oct. 26, 2015), https://www.hollandhart.com/checklist-for-business-associates [https://perma.cc/LKM6-HDCA].

79. Susan L. Marr & Richard Cahill, *Requests to Amend a Medical Record*, THEDOCTORSCOMPANY (Jan. 2016), https://www.thedoctors.com/articles/requests-to-amend-a-medical-record/ [https://perma.cc/9KDN-N5XJ]; 45 C.F.R. § 164.524(a)(1) (2018); *id.* § 164.526(a)(1–2) (2018) (if a provider feels the information in a medical record is accurate and complete, the provider does not have to amend the medical record). A large issue with the medical records amendment provision is the appeals process. For individuals without many resources, including low income individuals, the appeals process is burdensome and confusing. *See id.* § 160.306 (setting out procedural requirements for filing a complaint). Specifically,

request to amend medical data because a patient does not want it in their medical record is based on sound public policy and law.[80] It is important that a doctor can access all pertinent information when making a medical judgment. However, this calls into question whether sensitive topics—such as economic status, homelessness, and incarceration status—are beneficial to the healthcare decision-making process.

Unlike medical information (such as immunization history and surgical notes), SDH information can be ever-changing and less directly related to the quality of a patient's future medical care. Thus, if including this information is harmful, then patients should have the right to decide if this information is included in the medical record in the first place. If this information is beneficial, then patients should be able to manage the dissemination of information to other providers within the network. The failure of HIPAA to address the potential privacy harms of inserting SDH information into EHR within HIEs leaves individuals very little recourse. Unfortunately, neither federal nor state privacy laws offer much in the form of relief.

III. PRIVACY PROTECTIONS FOR SDH INFORMATION

HIPAA certainly allows SDH information explicitly disclosed by a patient to a medical professional to be placed into the patient's EHR and to be used in the same way as any other PHI.[81] Even if SDH information was disclosed via an external database (such as an HMIS) or deduced through the use of

---

because additional procedures for the filing of complaints can be noted in the Federal Register, *id.* § 160.306(b)(4), an individual other than an attorney or individual familiar with the Federal Register is less likely to be able to find the required procedures. While this is not the main thrust of my argument, it is an important consideration to keep in mind.

80. By deleting accurate information that truly does make a medical record more complete, the doctor is in danger of violating of the False Claims Act. This reflects public policy targeted at ensuring that medical records are kept accurate and complete. 31 U.S.C. §§ 3729(a)(1)(A), (B) (2012); Bald v. Kuakini Med. Ctr., No. CV 15-00525 RLP, 2017 WL 2117400, at *6 (D. Haw. Apr. 10, 2017) (stating that "medical records shall clearly and accurately document a patient's identity"); Thompson v. Mem'l Hosp. at Easton, Md., Inc., 925 F. Supp. 400, 405 (D. Md. 1996).

81. 45 C.F.R. § 160.103 (2018) (defining personal health information, covered entity, and business associate. A care coordinator is either a covered entity or a business associate, depending on the actual association with the patient's healthcare. Once sensitive information such as housing status or incarceration records is entered into a patient's EHR, it is protected by HIPPA).

public records and placed into an EHR with no opportunity for consent from the patient, current privacy laws allow much of that information to be used in the same way as any other PHI.[82] While HIPAA provides patients with a choice whether to disclose certain information to medical providers, the lack of privacy protections combined with the aggregation of data can largely negate that choice. Information drawn from public records is not protected by current medical record privacy laws because the information is not yet in a medical record. Additionally, information pulled from interagency databases (such as HMIS), while protected by partnership agreements and federal statute, is not subject to any overarching prohibition barring insertion into an EHR.[83] Therefore, a question of federal and state privacy law arises that goes beyond the narrow scope of medical records and HIPAA.

Although each piece of SDH information requires a slightly different analysis based on applicable federal and state laws, [84] this Comment will use housing status as an example of how this information should be analyzed when determining whether an HIE can obtain such information from an outside source. Based on current federal laws that allow anyone to utilize data found on a public record and allow government agencies to share sensitive information under certain federal provisions, the majority of SDH information can be obtained from outside sources and placed into an EHR without a patient's consent.[85] Because of inadequate privacy laws, there is no true limit on the processing of SDH information, allowing data to flow from one database to another without the knowledge or consent of the patient.

---

82. *Id.*; *see supra* Part II.

83. *See* Data and Technical Standards Final Notice, 69 Fed. Reg. 45,888, 45,888-903 (July 30, 2004).

84. For example, a doctor who wanted to know a patient's education status would have to comply with the Family Education Rights and Privacy Act as well as the Privacy Act of 1974, whereas a doctor who wanted to know a patient's past incarceration history would not have to deal with any specific privacy regulations. 20 U.S.C. § 1232g (Supp. V 2018); James B. Jacobs & Elena Larrauri, *Are Criminal Convictions a Public Matter? The USA and Spain*, 14 PUNISHMENT & SOC'Y 3 (2012).

85. *See infra* Section III.B. Keep in mind that, once this SDH information is placed into the EHR, it is protected by HIPAA and state medical record privacy laws. 45 C.F.R. pt. 160. This analysis will also be contingent on state law. *See infra* Section III.C.

In the context of housing status, Section A will first examine federal laws protecting the retrieval and use of housing status information. Section B will then turn to state laws pertaining to the use and dissemination of housing status information, focusing primarily on Colorado and California and the differences between them.

A. Privacy Act of 1974—Direct Distribution of SDH Information by Agencies

Without express consent by an individual, housing assistance information can be difficult to obtain directly from an agency—such as HUD, the federal agency that maintains records of every person within federal housing programs[86]—because of the protection afforded by the Privacy Act of 1974.[87] But it is not impossible. The Privacy Act provides that an agency[88] may not disseminate personally identifiable information about individuals without their consent unless the disclosure falls within one of twelve exceptions.[89] The exceptions include court orders, Freedom of Information Act disclosures, and statistical research.[90] The exceptions typically only apply to intra-agency disclosures or disclosures to other state or federal

86. *HUD's Public Housing Program*, U.S. DEP'T OF HOUSING AND URB. DEV., https://www.hud.gov/topics/rental_assistance/phprog (last visited Mar. 18, 2018) [https://perma.cc/85P3-42F4].

87. 5 U.S.C. § 552a (2012), *amended by* Pub. L. No. 113-295, 128 Stat. 4062 (codified at 5 U.S.C. § 552a(a)(8)(B)(viii)–(x) (Supp. V 2018)); *see also* U.S. Dep't of Housing and Urb. Dev. Office of Pub. and Indian Hous., NOTICE PIH-2014-10, Privacy Protection Guidance for Third Parties (Apr. 30, 2014), https://www.hud.gov/sites/documents/PIH2014-10.PDF [https://perma.cc/99UM-4UPE].

88. Agency is defined as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the [federal] Government (including the Executive Office of the President), or any independent regulatory agency." 5 U.S.C. § 552(f)(1) (2012).

89. *Privacy Act of 1974*, U.S. DEP'T OF JUSTICE, https://www.justice.gov/opcl/privacy-act-1974 (last visited Mar. 18, 2018) [https://perma.cc/BT9T-PZJJ]; 5 U.S.C. § 552a(b) (2012) (detailing twelve statutory exceptions, most of which apply to the release of information to other agencies or governmental entities that will affect the performance of those entity's duties); Big Ridge, Inc. v. Fed. Mine Safety & Health Review Comm'n, 715 F.3d 631, 650 (7th Cir. 2013).

90. *See* 5 U.S.C. § 552 (2012), *amended by* Pub. L. No. 114-185, 130 Stat. 538 (codified at 5 U.S.C. §552 (Supp. V 2018)). For an excellent breakdown of the twelve exceptions, see U.S. DEP'T OF JUSTICE OFFICE OF CIVIL LIBERTIES, OVERVIEW OF THE PRIVACY ACT OF 1974 54–115 (2015), https://www.justice.gov/opcl/file/793026/download [https://perma.cc/V2B6-FSA4].

agencies for specific purposes, such as emergencies or to determine the eligibility of an individual for other state- or federal-sponsored programs.[91]

Of the exceptions, only one, that of "routine use," might be relevant to the disclosure of federal housing assistance information for healthcare purposes.[92] The "routine use" exception applies to any "use of such record for a purpose which is compatible with the purpose for which it was collected" *and* which is published under "routine uses" in the Federal Register.[93] Although HUD does not currently have any such routine uses published in the Federal Register, the routine use exception typically allows the distribution of sensitive information to another agency for the purpose of determining eligibility for a state-sponsored program.[94] As HIEs become publicly owned rather than privately owned, the eligibility exception could leave a gap in privacy protection of SDH information if an agency such as HUD created a routine use exception for the data.

---

91. The broadest of the exceptions, 5 U.S.C. § 552a(b)(3), refers to "routine uses," which, although broad, has requirements that are intended to "discourage the unnecessary exchange of information . . . to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material." Christopher W. Wasson, *Privacy Law—The Routine Use Exception to the Privacy Act: A Clarification on Compatibility*, 35 VILL. L. REV. 822, 828–29 (1990) (quoting Britt v. Naval Investigative Service, 886 F.2d 544, 550 (3d Cir. 1989)). However, "routine uses" can include an agency giving sensitive information to another agency for the purpose of determining eligibility of a state sponsored program. Privacy Act of 1974 Report of New Routine Use, 60 Fed. Reg. 2,144 (Jan. 6, 1995). Therefore, if the HIE was a state sponsored HIE, this may be one way to obtain housing information from an agency like HUD. Other exceptions refer to use by Congress, 5 U.S.C. § 552a(b)(9), court order, 5 U.S.C. § 552a(b)(11), and to a consumer reporting collection agency per the Debt Collection Act, 5 U.S.C. § 552a(b)(12).

92. 5 U.S.C. § 552a(b)(3) (2012). When analyzing other SDH information, 5 U.S.C. § 552a(b)(8) may be pertinent. This exception allows an agency to disclose personal information pursuant to "compelling circumstances affecting the health or safety of an individual." *Id.* § 552a(b)(8).

93. 5 U.S.C. § 552a(a)(7) (2012); *id.* § 552a(e)(4)(D); *id.* § 552a(b)(3); U.S. DEP'T OF JUSTICE, *supra* note 90, at 83.

94. *See* HUD's Remedial Efforts in the Event of a Breach, 72 Fed. Reg. 52,572 (Sept. 14, 2007) (amended by Republication of HUD's Routine Use Inventory Notice, 80 Fed. Reg. 81,837 (Dec. 31, 2015)). The content amended by the Republication does not affect the analysis or conclusion of this discussion). Because routine use is agency-specific, each agency has different routine uses listed in the Federal Register and, depending on what information is being given out, a disclosure for medical care may fall within this exception.

If a care coordinator (e.g., a social worker)[95] is able to obtain a patient's housing status information through one of the Privacy Act exceptions, she could then make a note in the EHR that the patient was homeless or in transient housing. There are no federal laws that enable a patient to ensure the information is taken off her medical record.[96] At this point, the information has been shared and, regardless of whether the patient wants that information in the EHR or not, every doctor within the HIE can now see that the patient is homeless.

On the other hand, if the care coordinator obtains information from an agency without properly going through a Privacy Act exception, a patient can bring a claim under the Privacy Act.[97] The Privacy Act authorizes damages starting at $1,000 for an agency's intentional or willful failure to comply with the Act.[98] However, the patient would need to prove "some actual damages" in order to be successful.[99] Actual damages could be extremely difficult to prove if the patient received care from a provider but felt that the care was subpar, rushed, or otherwise unsatisfying. The difficulty in showing actual damages is further exacerbated by the fact that emotional distress alone does not qualify for relief, thus the patient would have to

---

95. This Comment uses the example of the care coordinator because the large HIE referred to in note 6 is primarily concerned with the care coordinator's ability to get the information. The following email is illustrative (edited for anonymity):

> "[D]octors don't want/need this; care coordinators do. As an example: A doc releases a patient after surgery with 2 meds and directions to get to physical therapy twice a week. It is on the care coordinator to help organize that. If the care coordinator knows there is a transportation issue, then 'just' getting meds and getting to physical therapy becomes problematic and the coordinator needs to be more creative with next steps (vouchers for [bus transportation], vouchers for Uber, etc.). And when that is not solvable/solved, the patient doesn't recover as expected/is readmitted unnecessarily (the $ side of that is that providers don't get their value-based payments in full)." This Comment focuses on the ability of the care coordinators to gather the information and place it in a patient's EHR. Once the information is in the EHR, future doctor bias (and subsequently potential lower quality of care) becomes an unintended side effect of the care coordinator's actions.

E-mail from Chief Strategy Officer, Anonymous Private HIE, *supra* note 14.

96. *See* sources cited *supra* note 79.

97. Stafford v. SSA, 437 F. Supp. 2d 1113, 1117–18 (N.D. Cal. 2006). It is often very hard to prove an exception to the general Privacy Act of 1974 rule. *See* 5 U.S.C. § 552a(g) (2012).

98. 5 U.S.C. § 552(g)(1)(D) (2012); *id.* § 552(g)(4)(A).

99. Doe v. Chao, 540 U.S. 614, 627 (2004).

prove that the care given was objectively harmful to the patient.[100]

Although it may be difficult to obtain SDH information from HUD directly, receiving information from an HMIS does not require an exception to the Privacy Act. In an HMIS, the data collection happens through a group of organizations in the community, not through HUD.[101] The group of organizations consists of private entities and nonprofit organizations, none of which are bound by the constraints of the Privacy Act. Therefore, housing information can be gathered either through an HMIS, if the healthcare system is a participating agency, or through public records, such as those found on the internet.

B. Federal Laws Controlling Distribution of SDH Information Through Public Records and Private Agreements

Even more concerning than the scattered protections given to SDH information housed in agency databases is the complete lack of protections afforded to information that is either already in the public record or disclosed through a private agreement. Privacy laws beyond the Privacy Act effectively allow information initially disclosed with the intent of one use—such as the disclosure of an address to receive mail through the USPS—to be used for any secondary purpose as long as no express contract is violated.

For example, although HUD may not be able to divulge information about a patient's housing status, an investigation into public records could reveal any combination of a patient's private information. A care coordinator who wants to understand whether a patient has stable housing could start by asking the patient for her address or looking for an address through insurance records (such as Medicare or Medicaid),[102]

---

100. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 678 (Rachel E. Barkow et al. eds., 6th ed. 2017).

101. 42 U.S.C. § 11360a (2012).

102. *See, e.g.*, *Qualifications for Medicaid in Colorado*, MEDICAID-HELP.ORG, https://medicaid-help.org/Colorado-Qualifications (last visited Mar. 18, 2018) [https://perma.cc/BR6J-URV3] (these federal programs require an address when confirming an individual's residence in the state and income).

arrest records,[103] or USPS records. Whatever the source, the care coordinator could then research the address using something as simple as Google Maps[104] and discover whether the address correlates with Section 8 housing, a halfway house, a church, or a home.[105] This may not be a common occurrence now, but as technology becomes more powerful, this type of searching could easily be automated using simple algorithms. Similarly, a care coordinator at an HMIS partner agency working with a patient in that community's HMIS has most of this information or has a statutory reason to collect it.[106] At this point, whatever information the care coordinator feels is pertinent to the patient's care can be placed in the patient's EHR, with or without the patient's consent. Once again, this Comment looks prospectively to the rapid evolution of technology and calls for a solution before the problem expands even further.

Because the Privacy Act protects information distributed among state and federal agencies and does not protect against private companies disclosing information, the only remaining federal claim an individual may have is a constitutional invasion of privacy claim.[107] However, this claim is only effective against state or federal agencies (i.e., government actors). Thus, an individual whose information was made available to hundreds of medical providers within a private HIE is left without recourse under federal law.

The Constitution provides a federal right to privacy, at least to some extent.[108] This right was first illuminated in

---

103. Arrest records can become public in various ways including disclosures through police blotters or a police department's sale of arrestee information to the public. JAMES B. JACOBS, THE ETERNAL CRIMINAL RECORD 194, 196 (2015).

104. *Google Maps*, GOOGLE, https://www.google.com/maps (last visited Jan. 15, 2018) [https://perma.cc/H8VR-BF38].

105. As an example, by typing in an address that is Section 8 housing, a website for Section 8 housing will often show up. For example, if you type in "951 arapahoe ave boulder co," a website indicating that this address is a Section 8 housing address will appear in the search options. *Google Search for 951 arapahoe ave boulder co*, GOOGLE, https://www.google.com/ (last visited Jan. 15, 2019) [https://perma.cc/Y8D5-NK85]. The first website that appears is *Arapahoe Court*, BOULDER HOUSING PARTNERS, https://boulderhousing.org/property/arapahoe-court [https://perma.cc/J7TR-RMUV].

106. 42 U.S.C § 11360a(f)(3) (2012).

107. Whalen v. Roe, 429 U.S. 589, 598–600 (1977); U.S. DEP'T OF JUSTICE, *supra* note 90, at 5; Implementation of Section 552a of Title 5 of the United States Code, 40 Fed. Reg. 28,949 (Jul. 9, 1975).

108. U.S. CONST. amend. XIV; U.S. CONST. amend. V.

Olmstead v. United States, where Justice Brandeis's dissent viewed the "right to be let alone" as a fundamental liberty.[109] Although Brandeis's view did not prevail in the decision, it did lay the foundation for *Griswold v. Connecticut*, which established a general right to privacy.[110] Since then, the Supreme Court has broken the right to privacy into two general categories: the "individual interest in avoiding disclosure of personal matters" and "independence in making certain kinds of important decisions."[111] The interest in avoiding disclosure of personal matters is most pertinent to a discussion of whether an HIE can disseminate housing status information to its network.[112]

The U.S. Supreme Court has yet to announce the framework under which a claim based on the right to avoid disclosure of personal matters should be analyzed. The Court has had a few chances since *Griswold*, but the question of which test to apply continues to leave lower courts baffled. In *United States v. Nixon*,[113] the Court balanced President Nixon's interest in keeping information confidential with the public's interest in having the information disclosed but ultimately "failed to take advantage of [the case] to clarify the test for evaluating informational privacy claims."[114] The Court came slightly closer in 2014, explaining that the distribution of a government background check targeting sensitive, personal information would be an invasion of privacy.[115] It heavily emphasized the reasonableness of the government's request and explained that the downstream privacy implications were protected by other statutes.[116]

Regardless, the constitutional right to privacy only protects individuals from government invasions within the "zone[] of privacy" covered by the Fifth and Fourteenth Amendments,

---

109. 277 U.S. 438, 478–79 (1928) (Brandeis, J., dissenting).

110. 381 U.S. 479 (1965); Paul Karlsgodt, *Tenth Circuit Survey: Civil Rights*, 73 DENV. U. L. REV. 671, 673 (1996).

111. *Whalen*, 429 U.S. at 598–600.

112. As such, this paper will not discuss the protection given to "independence in making certain kinds of important decisions." *Id.*

113. 433 U.S. 425, 464 (1977).

114. Scott Skinner-Thompson, *Outing Privacy*, 110 NW. U. L. REV. 159, 181 (2015).

115. NASA v. Nelson, 562 U.S. 134, 156–58 (2011).

116. Skinner-Thompson, *supra* note 114, at 183.

not from private entities.[117] Because HIEs are private, an individual could not bring a claim that the HIE violated her right to privacy.[118] Still, an analysis of the constitutional right to privacy is relevant when considering the impact on privacy should the United States achieve its vision of a nationwide HIE housed under a federal agency. The state action doctrine may also become relevant if states begin running or exercising significant control and involvement over HIEs in the future.[119]

In short, if a care coordinator retrieves an address from a public document or receives housing information by way of an HMIS and identifies that address as being indicative of transient or low-income housing, a note could be put into the EHR of an individual without any federal legal implications. This failure of our federal legal system leaves only state law for an individual to turn to.

C. State Laws Protecting Distribution of SDH Information

This Comment uses Colorado as an example of state law governing the distribution of SDH information. As with the federal privacy regime, an HIE can generally distribute any

---

117. Roe v. Wade, 410 U.S. 113, 152 (1973); Nilson v. Layton, 45 F.3d 369, 371 (10th Cir. 1995); U.S. CONST. amend. XIV; U.S. CONST. amend. V.

118. The "Due Process Clause of the Fourteenth Amendment protects individuals from state intrusion on fundamental aspects of personal privacy." *Nilson*, 45 F.3d at 371.

119. There is a symbiotic relationship when there is a sufficiently "'close nexus between the State and the challenged action' that seemingly private behavior 'may be fairly treated as that of the State itself.'" Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass'n, 531 U.S. 288, 295 (2001) (citing Jackson v. Metro. Edison Co., 419 U.S. 345, 349 (1974)). At that point, the court would run through a three-part test created in *Denver Policemen's Protective Ass'n v. Lichtenstein* that asks "(1) if the party asserting the right has a legitimate expectation of privacy, (2) if disclosure serves a compelling state interest, and (3) if disclosure can be made in the least intrusive manner." 600 F.2d 432, 435 (10th Cir. 1981). An additional consideration when making this inquiry is whether the "derivative theory" could be used as a defense against HUD having to produce such documents. U.S. Dep't of State v. Ray, 502 U.S. 164 (1991) (Scalia, J., concurring). States are entering the HIE marketplace, albeit slowly. Jacqueline LaPointe, *Small Number of States Successful with State-Led HIE Use*, EHR INTELLIGENCE, https://ehrintelligence.com/news/small-number-of-states-successful-with-state-led-hie-use (last visited Jan. 20, 2019) [https://perma.cc/L8KU-59ZY]; *see also Status of Health Information Exchanges: 50 State Comparison*, HEALTH INFO. & L., http://www.healthinfolaw.org/comparative-analysis/status-health-information-exchanges-50-state-comparison (last updated Dec. 13, 2013) [https://perma.cc/2W4H-A39F].

public information to its network without violating a Colorado resident's privacy rights. That is, there are no specific statutes protecting the dissemination of information deduced from public records.[120]

The tort of invasion of privacy can be used in certain situations where SDH information is distributed without an individual's consent. In general, the tort of invasion of privacy includes four typical claims: (1) intrusion upon an individual's seclusion or private affairs, (2) public disclosure of private facts, (3) appropriation of an individual's name or likeness, and (4) publicity that places an individual in a false light.[121] However, each state can choose which of these claims to recognize, and many do not recognize one or more.[122] Colorado, for example, recognizes three of the four claims for invasion of privacy, rejecting only the tort of false light.[123] The application of the privacy torts are limited to when (1) consent was given for the initial disclosure or (2) when the information is in a public record.[124] Therefore, this Comment will give a brief overview of the privacy torts in this specific context.

When gathering information, HMISs are initially required to get consent from an individual for the dissemination of their information.[125] An individual's consent typically allows the information to be entered into the HMIS database and shared with all partner agencies.[126] But these consent forms fre-

120. *See generally* DAVID M. STRAUSS & GREGORY P. SZEWCZYK, COLORADO PRIVACY AND SECURITY HANDBOOK (2017).

121. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

122. Denver Publ'g Co. v. Bueno, 54 P.3d 893, 896 (Colo. 2002) ("Whether to adopt [the four categories of invasion of privacy claims] as viable tort claims is a question of state law.").

123. *Id.* at 903.

124. For a comprehensive examination of the usefulness of the privacy tort in the digital ago, see Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805 (2010).

125. BROOKE SPELLMAN ET AL., CENT. FOR SOC. POL'Y, JOHN W. MCCORMACK INST. OF PUB. AFF., HOMELESS MANAGEMENT INFORMATION SYSTEMS: IMPLEMENTATION GUIDE 18 (2002), https://safehousingpartnerships.org/sites/default/files/2017-01/implementationguide.pdf [https://perma.cc/5BJW-62UL]; 7A COLO. PRAC., PERSONAL INJURY TORTS AND INSURANCE § 33:14 (3d ed. 2018).

126. *See, e.g.*, *Homeless Management Information System (HMIS) Consumers Informed Consent & Release of Information Authorization*, SACRAMENTO STEPS FORWARD, https://sacramentostepsforward.org/wp-content/uploads/2018/01/HMIS-Consumers-Informed-Consent-Release-of-Information-Authorization.pdf (last updated June 5, 2016) [https://perma.cc/CRP2-ABPF]; Salvador Munoz, *Client Consent and Supplemental (ROI)*, ALLCHICAGO, https://hmis.allchicago.org/hc/en-

quently do not include a list of participating agencies, though they offer a list upon request.[127] Even if the consent forms did include a list of each partner agency within the HMIS, such a list would not have information on all of the members of an HIE that an HMIS healthcare partner may also be part of. Unfortunately, with America's "one bite at the apple" concept of consent, the initial consent is enough to pull an individual's privacy harm out of the realm of tort law.[128]

Similarly, information gathered from public records is typically unprotected from use that was unintended at the time of initial disclosure, especially when the unintended use simply restates true and accurate information. Indeed, the three Colorado privacy claims governing the dissemination of accurate information—intrusion upon an individual's seclusion or private affairs, public disclosure of private facts, and appropriation of name or likeness—are useless to patients whose public information has been processed for an unintended secondary use.[129]

Specifically, a claim for intrusion upon seclusion will likely fail if a care coordinator uses information pulled from public records. The Restatement of Torts explicitly rejects an intrusion upon seclusion claim based on already public information, stating that "there is no liability for the examination of a public record concerning the plaintiff."[130] Relatedly, a claim for public disclosure of private facts will also fail if the information is pulled from public records. The general rule is: if someone gives further publicity to an already-public fact, there is no invasion of privacy.[131] The Restatement gives examples of already-public information, such as dates of birth, marriage licenses,

---

us/articles/360000825243-Client-Consent-and-Supplemental (last visited Oct. 12, 2018) [https://perma.cc/2ESV-8V9H].

127. *See, e.g.*, *Homeless Management Information System (HMIS) Consumers Informed Consent & Release of Information Authorization*, *supra* note 126; Munoz, *supra* note 126. Once again, the issues with an HMIS are beyond the scope of this Comment but it is interesting to consider the implications of homeless individuals signing a consent form that has a large portion of the information lacking or available "upon request."

128. The United States' approach to consent is discussed further in the conclusion. *Supra* Section IV.A.

129. *See* RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 2018); *id.* § 652D, Special Note on Relation of § 652D to the First Amendment to the Constitution; *id.* § 652B.

130. RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (AM. LAW INST. 2018).

131. RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (AM. LAW INST. 2018); Robert C. Ozer, P.C. v. Borquez, 940 P.2d 371, 377 (Colo. 1997) ("The disclosure of facts that are already public will not support a claim for invasion of privacy.").

military records, and lawsuit pleadings.[132] Colorado courts apply this broad interpretation when considering the viability of claims for invasion of privacy for public disclosure of private facts.[133] Finally, a claim for appropriation of name or likeness is only applicable in situations where the defendant uses the name or likeness of another for the defendant's interest and without the consent of the individual.[134] This claim is likely inapplicable in this situation and is therefore beyond the scope of this Comment.

Thus, if a care coordinator finds a correct address through arrest records, the USPS, or any other public source and correctly assumes an individual is homeless or in low-income housing, this information could be entered into the EHR without the individual's permission and disseminated to other care providers within the network without being subject to a claim for invasion of privacy.

Even more disturbing than the lack of Colorado state law protections for the distribution of correct information is the dearth of protections for the dissemination of incorrect information. Out of the four generally recognized torts of invasion of privacy, the only claim that may apply to the dissemination of incorrect information is "false light."[135] As noted above, false light claims are not recognized in Colorado.[136] Thus, a patient whose care coordinator incorrectly assumed the patient was homeless and placed this assumption into the EHR has no recourse through typical tort claims. As a last-ditch effort, a patient with no other options may attempt to bring a claim for

---

132. RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (AM. LAW INST. 2018); *see also* Aquino v. Bulletin Co., 154 A.2d 422, 427 (Pa. Super. Ct. 1959) (holding that "[t]here is no unwarranted invasion of a right of privacy in the description of a wedding even though it is intended to be entirely private").

133. *Robert C. Ozer, P.C.*, 940 P.2d at 377; Tonnessen v. Denver Publ'g Co., 5 P.3d 959, 966 (Colo. App. 2000).

134. Joe Dickerson & Assocs., LLC v. Dittmar, 34 P.3d 995, 1001 (Colo. 2001). The elements of this claim are:

> (1) the defendant used the plaintiff's name or likeness; (2) the defendant sought to take advantage of the plaintiff's reputation, prestige, social or commercial standing, or any other value attached to the plaintiff's name, likeness, or identity; (3) the use of the plaintiff's name or likeness was for the defendant's own purposes or benefit, commercially or otherwise; (4) damages; and (5) causation.

Id.

135. JACOBS, *supra* note 103.

136. SOLOVE & SCHWARTZ, *supra* note 100.

defamation.[137] This effort, while admirable, will still likely fail and ultimately be counterproductive, exposing the very information a patient seeks to keep private.

The Colorado Supreme Court defines defamation as "a communication that holds an individual up to contempt or ridicule thereby causing him to incur injury or damage."[138] This definition builds on the premise that statements are defamatory if they "tend[] so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him."[139] Libel is the specific form of defamation that encompasses false claims that are written down and disseminated.[140] To bring a libel claim, an individual must prove the elements of defamation as well as plead and prove special damages.[141] Importantly, in both defamation and libel claims, the plaintiff has the burden of proving the elements and, in libel claims, must prove that the disclosure caused "special harm."[142]

In our hypothetical situation where a care coordinator put an incorrect notation in a patient's EHR that stated the patient was homeless, the underlying defamation claim would likely fail because the patient would be hard-pressed to show harm to her reputation in the estimation of the community. As defined

---

137. Keohane v. Stewart, 882 P.2d 1293, 1297 (Colo. 1994).

138. *Id.*

139. Burns v. McGraw-Hill Broad. Co., 659 P.2d 1351, 1357 (Colo. 1983) (quoting RESTATEMENT (SECOND) OF TORTS § 559 (AM. LAW INST. 1976)).

140. *Defamation, Slander and Libel*, NOLO, https://www.nolo.com/legal-encyclopedia/defamation-slander-libel (last visited Nov. 15, 2017) [https://perma.cc/G4NZ-MWPJ]. This explanation is truncated to fit the needs of the analysis. For a more in-depth look into libel see *Defamation Law Radio: Defamation Per Quod v. Defamation Per Se* (Traverse Legal broadcast July 27, 2012), https://www.traverselegal.com/blog/defamation-per-quod-vs-defamation-per-se/ [http://perma.cc/KXR9-8CTL]; RESTATEMENT (SECOND) OF TORTS § 570 (AM. LAW INST. 1977); 7A COLO. PRAC., PERSONAL INJURY TORTS AND INSURANCE § 32:16 (3d ed. 2017); Sunward Corp. v. Dun & Bradstreet, Inc., 811 F.2d 511, 517 (10th Cir. 1987); Denver Publ'g Co. v. Bueno, 54 P.3d 893, 898 (Colo. 2002) (citing BLACK'S LAW DICTIONARY 417 (6th ed. 1990)). The other type of defamation is slander—which is defamation spoken by the defendant. This claim is not applicable to this Comment. Marianne Bonner, *Defamation, Libel and Slander*, BALANCE, https://www.thebalance.com/defamation-libel-and-slander-462650 (last updated Oct. 30, 2017) [https://perma.cc/K7Y8-4A5R].

141. 7A COLO. PRAC., PERSONAL INJURY TORTS AND INSURANCE § 32:17 (3d ed. 2017). Special damages include "specific monetary losses that a plaintiff incurs as a result of the publication of statements or pictures by a defendant." *Id.*

142. *Sunward Corp.*, 811 F.2d at 518–19 (citing RESTATEMENT (SECOND) OF TORTS § 613 (AM. LAW INST. 1977)).

in the Restatement and adopted by Colorado courts, "community" does not necessarily mean the public at large; "it is not enough that the communication would be derogatory in the view of a single individual or a very small group of persons."[143] Thus, a patient who loses the respect of a single doctor or small group of healthcare providers within the HIE may be damaged but may not be able to prove that her reputation was harmed as to the estimation of the community.[144]

Colorado libel cases have closely examined the requirement of harm and generally require special damages to be laid out for each harm claimed.[145] Additionally, Colorado courts have adopted the Restatement's approach: to show special damages, it may be necessary to prove that the defamatory comment was received and understood as defamatory by the recipient.[146] "It is not enough that the language used is reasonably capable of a defamatory interpretation if the recipient did not in fact so understand it."[147] Going back to our hypothetical situation, the patient would have to show that the notation of homelessness was capable of being defamatory *and* that the doctors who received the notation understood it to be defamatory.[148] This is difficult for the patient to do because this burden is not satisfied by speculation alone and instead requires evidence of the recipient's actual understanding.[149]

The above analysis highlights the inadequate privacy protections afforded to homeless patients who do not want their housing status disclosed to a medical provider. A care coordinator likely faces no legal consequences if she takes an address

143. Bustos v. A&E Television Networks, 646 F.3d 762, 765 (10th Cir. 2011) (The court especially rejects a view from a very small group whose standards are improper. "Neither do we measure this comparative impact . . . from the viewpoint of any . . . insular group whose reactions may be different than the mainstream of contemporary society."); RESTATEMENT (SECOND) OF TORTS § 559 cmt. e (AM. LAW INST. 1977).

144. *Bustos*, 646 F.3d at 765 ("[A] misstatement is not actionable if the comparative harm to the plaintiff's reputation is real but only modest."); *cf.* Burns v. McGraw-Hill Broadcasting Co., Inc., 659 P.2d 1351, 1357 (Colo. 1983) (holding that a statement broadcasted to the public at large was defamatory).

145. Bernstein v. Dun & Bradstreet, Inc., 149 Colo. 150, 153 (1962); Knapp v. Post Printing & Publ'g Co., 111 Colo. 492, 499 (1943).

146. *Sunward Corp.*, 811 F.2d at 519; RESTATEMENT (SECOND) OF TORTS § 559 cmt. d (AM. LAW INST. 1977).

147. *Sunward Corp.*, 811 F.2d at 519 (citing RESTATEMENT (SECOND) OF TORTS § 613 (AM. LAW INST. 1977)).

148. *Id.*

149. *Id.*

from a public record or a state agency, places a correct or incorrect assumption about a patient's housing status in an EHR, and disseminates that information to an entire network of medical providers within an HIE. In our current system, the homeless patient has no choice and no control over who within the medical system knows that she lacks stable housing.

IV. SOLUTION

Current privacy laws do not adequately protect an individual's SDH information from inappropriate use in an EHR. Between the federal push toward the integration of databases and a dearth of federal and state regulations protecting against the use of public records to gain information, at-risk individuals can become subject to severe privacy intrusions.[150]

Whether a person is in transient housing, has a criminal record, or uses food stamps, SDH information can potentially be embarrassing for the individual and can ultimately lead to lower quality of care if divulged to the wrong healthcare provider.[151] While this is not to say that sensitive SDH information should never be used, the processing of that data should be limited by agreements prior to the entry of the data into a record, and each new use of the data should be controlled by the individual. If a care coordinator would like to gather information from public records or use information assembled in an HMIS database to ensure that the individual gets higher quality care, the care coordinator should first reach out to the individual and ask for permission to use the data in the healthcare context. In essence, the use of SDH information in an EHR should hinge on whether a patient gives explicit permission for its use in that particular manner or not. This Comment proposes a menu of solutions that include (1) broad, overarching federal privacy regulation, (2) sector-specific privacy regulation, (3) state-based privacy regulation, and (4) a quick fix.

150. *Supra* Part I.
151. *See supra* Introduction.

A. Overarching Federal Privacy Regulations

An obvious solution to the improper secondary use of SDH in EHR is to enact an overarching federal privacy regime that can target both government agencies and private entities. An omnibus privacy law could prohibit a care coordinator from inserting information into an EHR unless a patient either voluntarily gives the care coordinator the information or voluntarily consents to a secondary use of the SDH information (e.g., from the HMIS into the EHR). By enacting legislation authorizing this type of regulation, information can be protected both before and after it enters an EHR.

The United States is often criticized for its lack of a complete data privacy law.[152] Many argue that this stems from an emphasis on a "collect everything" mentality for commerce and national security purposes rather than respecting personal data as something owned by citizens.[153] Although an argument may be made that federal privacy regulations that target private entities and allow for a private causes of action could staunch economic growth, a counterargument can be made by looking to California. With the strictest privacy regulations in the country (that target private entities), California is still ranked third in the country for the strength of its economy.[154] Thus, even in the United States, we can implement privacy laws that do not staunch commerce and still protect our citizens.[155]

---

152. STEPHEN COBB, DATA PRIVACY AND DATA PROTECTION: US LAW AND LEGISLATION 2 (2016).

153. *Id.*

154. Samantha Sharf, *The States With The Best and Worst Economies*, FORBES (June 6, 2016, 1:49 PM), https://www.forbes.com/sites/samanthasharf/2016/06/06/the-states-with-the-best-and-worst-economies/ [https://perma.cc/T3XF-ZM7F] (noting that much of California's economy is built through its venture capital and tech jobs, which indicates that state privacy regulations have not stymied commercial growth in these sectors); COBB, *supra* note 152, at 3.

155. It is yet to be determined how California's newest privacy law, the California Consumer Privacy Act (CCPA), will affect industry in California. The CCPA is similar to the EU's General Data Protection Regulation (GDPR) in that it declares privacy an "inalienable right" and lays down a series of rights that California citizens have in regard to their data. The bill goes live on January 1, 2020. Assem. Bill 375, 2017–2018 Reg. Sess., ch. 55 § 2 (Cal. 2018). *See generally* Assem. Bill 375, 2017–2018 Reg. Sess. (Cal. 2018); *About the California Consumer Privacy Act*, CALIFORNIA CONSUMER PRIVACY ACT, https://www.caprivacy.org/about (last visited Oct. 14, 2018) [https://perma.cc/38ZH-7MS4].

To achieve a federal privacy regime, Congress should look to the EU as a model of stricter privacy laws that protect citizens over corporations.[156] The European Convention on Human Rights took the stance in 2010 that every person has a "right to respect for his private and family life, his home and his correspondence."[157] Since then, EU courts have interpreted "private life" broadly to include data and discourage the collection of stored data without an individual's consent.[158] Additionally, the EU's General Data Protection Regulation (GDPR), which deemed privacy a "fundamental right," went into force on May 25, 2018, and legally strengthened the EU's commitment to privacy.[159] Unlike the United States's piecemeal privacy legislation that is restricted to particular sectors and situations, the EU's GDPR protects an individual's personal data from all types of involuntary use and misuse (barring a few stated exceptions), regardless of sector or situation.[160]

Although there are many benefits to fully adopting a GDPR-style regime, this Comment addresses a very narrow issue that could be solved primarily through federal definitions of key privacy terms and universal requirements of notice and

---

156. *Protection of Personal Data*, EUROPEAN COMM'N, https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en (last visited Feb. 16, 2019) [https://perma.cc/5QUZ-W2VP]. At this point, the United States can also look to other countries that have adopted the GDPR, such as Brazil. *See* Renato Leite Moneteiro, *The New Brazilian Data Protection Law—A Detailed Analysis*, IAPP (Aug. 15, 2018), https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/ [https://perma.cc/Z5LY-CZUC].

157. Eur. Council, *European Convention for the Protection of Human Rights and Fundamental Freedoms*, Art. 8 (2010), https://www.echr.coe.int/Documents/Convention_ENG.pdf [https://perma.cc/EQY9-49T7].

158. Marc Rotenberg & David Jacobs, *Privacy, Security, and Human Dignity in the Digital Age: Updating the Law of Information Privacy: The New Framework of the European Union*, 36 HARV. J.L. & PUB. POL'Y 605, 611 (2013). *See generally* COBB, *supra* note 152, at 3.

159. Commission Regulation 2016/679, rec. 1, 2016 O.J. (L 119) 1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX.32016R0679 [https://perma.cc/V7AZ-CKW7] [hereinafter GDPR].

160. COBB, *supra* note 152, at 3. Rotenberg & Jacobs, *supra* note 158, at 611. Current United States privacy law is heavily influenced by commercial lobbyists. The Privacy Act of 1974 was intended to include both state agencies and private enterprises. However, through efforts of lobbyists representing commercial interests, the final law limited the scope of the legislation to federal agencies. COBB, *supra* note 152, at 3.

consent. Thus, this Comment argues for a more nuanced approach to overarching federal regulation.

Congress should enact a federal privacy regime that simply creates definitions for key terms in existing federal privacy legislation. Focusing on terms such as "data," "notice," and "consent" would enable citizens to regain control over their data and also help companies, agencies, and citizens better comply with the patchwork of privacy laws in the United States.

For an example of the mismatched definitions issue and how a less intrusive federal privacy regime would impact current practices, compare HIPAA with the McKinney-Vento Act. In HIPAA, the definition of "personally identifiable information" (the "data") includes "information that is a subset of health information, including demographic information collected from an individual" that relates to the provision of past, present, or future healthcare.[161] On the other hand, the McKinney-Vento Act does not define "data" in an HMIS at all.[162] Instead, the Act punts many of the specifics to the Secretary who, in turn, punts the definition and requirements of data security to each individual HMIS.[163] Thus, "data" definitions are different from HMIS to HMIS, all of which differ from the definition of "data" in HIPAA.[164]

The different definitions of "consent" provide another example. The idea of consent, defined as "authorization" in HIPAA, requires a person's written, signed agreement for the disclosure of PHI.[165] Although authorization (consent) is defined under HIPAA and requires specific protections for an individual, the term "consent" is not defined in the McKinney-Vento Act.[166] Thus, definitions that are completely inconsistent

---

161. 45 C.F.R. § 160.103 (2018). The information must also be created by an employer, health care provider, health plan, or health care clearinghouse. *Id.* An overview of some types of information specifically protected can be found in *Protected Health Information: HIPAA PHI*, COMPLIANCY GROUP, https://compliancy-group.com/protected-health-information-understanding-phi/ (last visited Oct. 14, 2018) [https://perma.cc/LU2M-GVAJ].

162. *See* 42 U.S.C. § 11360 (2012).

163. *Id.*; 76 Fed. Reg. 76,919–20 (Dec. 9, 2011).

164. 42 U.S.C. § 11360; 76 Fed. Reg. 76,919–20 (Dec. 9, 2011) (codified at 24 C.F.R. pt. 91, 576, 580, 583); Daniel L. Macioce, Jr., *PII in Context: Video Privacy and a Factor-Based Test for Assessing Personal Information*, 45 PEPP. L. REV. 331, 344–45 (2018).

165. SOLOVE & SCHWARTZ, *supra* note 100, at 515.

166. *Id.*; 45 C.F.R. § 164.506(b) (2018); 42 U.S.C. § 11360.

or altogether nonexistent take the control of personal data completely out of the hands of the individual and put it squarely into the hands of federal agencies.

A federal privacy law that defines key privacy terms and provides that any federally funded programs must have a notice and consent requirement would at least put a floor in place for U.S. citizens' privacy protections. For example, if a new federal privacy regulation took the language of "consent" from the GDPR, organizations would be required to obtain consent through "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[167] The definition of "consent" would then be applied to every existing federal (and perhaps even state) privacy law. These harmonized definitions, combined with a notice and consent requirement for federally funded organizations that deal with data collection or processing, would give citizens more control over the processing of their data and effectively create a processing limitation.[168]

To put a finer point on why this type of federal privacy regulation may be adequate, at least in the short term, take the example of a homeless individual involved in an HMIS. The McKinney-Vento Act could only fund organizations that collect and process data per the requirements of the regulation.[169] Currently HUD simply requires that an individual give "oral or written consent" before any information is collected by an HMIS.[170] However, enormous leeway is given to organizations to craft notices and consents based on an organization's own uses.[171] This vague requirement of notice and consent empow-

167. GDPR, *supra* note 159, art. 4(11).

168. The term "processing limitation" can be understood as a subtype of "use limitation" that focuses primarily on how the data flows, rather than how the data is used. For a broader discussion of "use limitations," see Kevin P. McLaughlin, *Sharing You with You: Informational Privacy, Google, & the Limits of the Use Limitation*, 23 ALB. L.J. SCI. & TECH. 55 (2013).

169. 69 Fed. Reg. 45,891 (July 30, 2004).

170. ABT ASSOCS., INC., *supra* note 40, at 12.

171. *Id.* at 12, 22–29. The sample notice given by HUD goes so far as to explain that the consent an individual gives is "for the purposes described here and *for other uses and disclosures that we determine to be compatible with these uses or disclosures.*" *Id.* at 24 (emphasis added).

ers partner organizations to use the data in very different ways.

Conversely, with federal definitions of "notice" and "consent" in place, an individual would go to an HMIS partner agency (such as a job interview training organization) and consent to a very specific use of her data. The consent form would follow requirements similar to the GDPR and provide explicit and unambiguous information regarding where the data is going and what it will be used for.[172] If the consent form did not include a provision allowing the information to be entered into an EHR, the information would not be entered into an EHR—neither by way of direct data integration nor as piecemeal entry by the healthcare provider or care coordinator. Further, even if the consent form did allow for the entry of data into an EHR, this might not include transmission into an HIE. For the data to be transferred into an EHR that is part of an HIE, further consent would be required. Essentially, instead of an individual having a single opportunity to consent to the release of personal information, an individual would now have to give consent for each additional use of the data beyond the original purpose consented to.[173]

A basic floor of privacy regulations still leaves much to be desired. First, it may not satisfy the GDPR's requirement of "adequate" privacy protections for international data transfers.[174] Additionally, it would not give individuals a private right of action. The lack of a private right of action for privacy protections may lead to higher enforcement costs for the federal government and lower incentives for companies to comply quickly and adequately with the requirements.[175] In the end, fully fleshed-out privacy regulation is likely the best option. But in the current congressional climate, it may make sense to take privacy one step at a time—allowing Congress to watch

---

172. *See* Andrew Clearwater & Brian Philbrook, *Practical Tips for Consent Under the GDPR*, IAPP (Jan. 23, 2018), https://iapp.org/news/a/practical-tips-for-consent-under-the-gdpr/ [https://perma.cc/4ZRV-CL9M].

173. *Cf.* GDPR, *supra* note 159, rec. 32 ("When the processing has multiple purposes, consent should be given for all of them.").

174. *Id.* at art. 45.

175. *See* Bradyn Fairclough, *Privacy Piracy: The Shortcomings of the United States' Data Privacy Regime and How to Fix It*, 42 J. CORP. L. 461, 478 (2016); James T. O'Reilly, *Deregulation and Private Causes of Action: Second Bites at the Apple*, 28 WM. & MARY L. REV. 235, 248 (1987) ("Private initiation suits cost agencies more time and money than do private rights of action.").

states demonstrate what does and does not work and to build privacy regulations that afford broader protections based on the results.

B. Sector-Specific Federal Privacy Regulations

Although an omnibus federal privacy regime would offer the highest protections for American citizens, a federal law with that scope may be unrealistic, as Congress arguably lacks both the expertise and the bandwidth to tackle a problem as complicated and substantial as a federal privacy law.[176] There are many issues to consider when passing a broad-reaching privacy law, including issues of federal preemption, First Amendment protections, and divergent sectoral privacy laws.[177] Thus, a realistic question to ask is: How can the United States adequately protect citizens' privacy without reinventing the wheel? That is, how can the United States use the current regulatory structure to protect SDH information from secondary use in an EHR and HIEs without an individual's explicit consent?

Perhaps the answer is to start with more discreet federal legislation and rulemaking that addresses the narrow issue highlighted in this comment: the privacy harms associated with processing SDH information. While an individual may consent to the insertion and subsequent processing of SDH in an HMIS, an individual may never have consented to (or understood her consent to encompass) the use of that same information in an EHR, much less an EHR in an HIE. Similarly, although an individual may give a care coordinator her address, the purpose of that disclosure would be to identify a place to send mail, not to allow an assumption about housing status that is subsequently entered into the EHR.

If the United States addresses the concepts of control and consent related to the processing of data before that data enters medical records, it could curtail the improper use of

176. Brendan Bordelon, *Split Congress Complicates Impending Privacy Push*, NAT'L J. (Nov. 8, 2018), https://www.nationaljournal.com/s/674513/split-congress-complicates-impending-privacy-push [https://perma.cc/V4QB-YGAP].

177. Robert Gellman, *One Way to Solve the U.S. Privacy Law Dilemma: An Opt-in Privacy Law*, IAPP (Oct. 12, 2018), https://iapp.org/news/a/one-way-to-solve-the-u-s-privacy-law-dilemma-an-opt-in-privacy-law/ [https://perma.cc/4DCE-6LCP]; SOLOVE & SCHWARTZ, *supra* note 100, at 140–64.

SDH in an HIE-housed EHR. As this Comment acknowledges, the use of SDH can be extraordinarily beneficial to the care provided to an individual by her healthcare team.[178] However, the disclosure of certain information can also lead to stigma and bias. An ideal processing limitation of SDH takes both sides into consideration and balances the need to know with the need to protect. A sector-specific solution could come in the form of legislation in which Congress amends HIPAA to directly address SDH information or a rulemaking option in which the Department of Health and Human Services (HHS) directly modifies the HIPAA Privacy Rule standards.

Unlike a federal omnibus law, an amendment to HIPAA could directly target the specific issue of SDH information in EHR by limiting the amount of information visible to physicians if there is no "need to know" or explicit consent. The obvious difficulties in this type of solution are (1) how to shield specific information from the view of the physician while still allowing other information to be visible and (2) determining whether the physician does, in fact, need to know the information. Laws preventing discrimination in the employment context offer models that could be applied to SDH information entering the medical record space. For example, the Genetic Information Nondiscrimination Act makes it unlawful for an employer to request genetic information from an employee or applicant in most situations.[179] However, the law provides exceptions for those instances when the employer needs to know the information.[180] In a similar fashion, HIPAA could limit what a provider may view when providing care to a patient.

To balance this limitation and allow the information to enter an EHR when useful or necessary, the amendment could allow a coordinator of care (such as a social worker) to view the information and make certain data visible to the provider when needed. The basis of the care coordinator's decision would need to stem from predetermined guidelines set by HHS outlining when it is appropriate to disclose SDH without a patient's ex-

178. *See supra* Section I.B.

179. 42 U.S.C. § 2000ff-1(b) (2012).

180. *Id.* This includes situations where the employer conducts DNA analysis and needs to know employee "DNA identification markers for quality control to detect sample contamination" or where the information is used to monitor the biological effects of toxic substances in the workplace. *Id.* § 2000ff-1(b)(5)–(6).

plicit consent. The ability of the care coordinator to step into the patient's role of consenter would create a privacy proxy that would help balance the knowledge gap between the healthcare provider and the patient regarding necessary health data and the patient's privacy. So, if the provider wanted the SDH information, he could access it in one of two ways: (1) the patient is informed of the proposed disclosure and has an opportunity to affirmatively object to that disclosure or (2) the patient's care coordinator concludes, based on predetermined guidelines, that the information would be beneficial to the actual treatment by the provider. Thus, this would effectively create one more step between the patient and the provider when nonmedical (SDH) information is in question, while substantially preserving the current system of medical information disclosure to providers.

An alternative to waiting for congressional action is to allow HHS to take point on the issue. HHS has the ability to modify the HIPAA Privacy Rule via rulemaking once every twelve months.[181] The HIPAA Privacy Rule is the regulation under HIPAA that details how HIPAA protects the privacy of patients' medical records, including limitations and requirements for disclosure, notice, and release.[182] Using its rulemaking authority, HHS could adjust the disclosure requirements to limit data visible to a provider to only medical information while putting additional consent requirements on nonmedical (SDH) information, as outlined above. This may be a more logical option because the disclosure requirements could also incorporate the predetermined guidelines that permit care coordinators to disclose nonmedical information to providers.

This solution would only work if current EHR technology adapts to the bifurcation of nonmedical (SDH) information and medical information. The software would need to have the ability to show one set of data points to providers and another to care coordinators serving as privacy proxies. Then the software would need to allow the privacy proxy to switch on the visibility of specific data points when one of the two requirements for disclosure is met. Although ambitious, technological

181. *Will the Department of Health and Human Services (HHS) Make Future Changes to the HIPAA Privacy Rule and, if so, How Will These Changes Be Made?*, U.S. DEP'T OF HEALTH & HUM. SERV., https://www.hhs.gov/hipaa/for-professionals/faq/195/will-future-changes-be-made-to-the-hipaa-privacy-rule-if-so-how/index.html (last updated July 26, 2013) [https://perma.cc/85NP-ZKM9].

182. *See* 45 C.F.R. §§ 164.500–164.534 (2018).

changes in the medical record space are not unheard of, and Congress could certainly create incentives for the adoption of EHR software that incorporates this type of data segregation.[183] Congress or HHS would also need to outline a general list of what constitutes "nonmedical information" and determine what situations would allow a care coordinator to disclose nonmedical information to a physician without prior patient consent.

C. Suggestions for State Regulatory Reform

While waiting for Congress to implement new federal laws, states should pass citizen-friendly privacy laws. For example, states like Colorado could enact laws that bolster individuals' rights with respect to their medical records. As a supplement to HIPPA, California's Patient Access to Health Records Act (PAHRA) gives individuals the right to see and copy their own medical records (with certain restrictions) and request addendums if they feel the records are incorrect.[184] The primary benefit PAHRA provides individuals is a private right of action against healthcare providers if an individual's information is inappropriately distributed.[185] The ability to bring a claim gives individuals greater control over sensitive information in their medical records. Thus, an individual who is homeless or experiences another difficult situation may bring a private suit if she feels that her information was inappropriately used or disclosed.[186]

---

183. The HITECH Act is a law passed for the primary purpose of promoting the adoption of EHR and other meaningful use technology. *HITECH Act Enforcement Interim Final Rule*, U.S. DEP'T OF HEALTH & HUM. SERV., https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html (last updated June 16, 2017) [https://perma.cc/77ZW-7NN9]. A study on the effectiveness of the HITECH Act showed that the incentive structure of the law likely had a large impact on adoption rates. Julia Adler-Milstein & Ashish K. Jha, *HITECH Act Drove Large Gains in Hospital Electronic Health Record Adoption*, 36 HEALTH AFF. 1416 (2017), https://www.healthaffairs.org/doi/full/10.1377/hlthaff.2016.1651 [https://perma.cc/KT22-LHCY].

184. CAL. HEALTH & SAFETY CODE §§ 123100–123149.1 (West 2019); CAL. HEALTH & SAFETY CODE § 123111 (West 2019); *Health and Medical Privacy Laws (California Medical Privacy Series)*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/consumer-guides/health-and-medical-privacy-laws-california-medical-privacy-series (last updated Oct. 2, 2017) [https://perma.cc/CGU7-DFL7].

185. CAL. CIV. CODE § 56.36(b) (West 2019).

186. It is still questionable whether someone in a poor socioeconomic situation would have the means to bring a suit against a wrongdoer. Such discussion is

Although a law such as PAHRA would offer some relief, it is directed at private parties and does not address information misuse by state agencies. Thus, Colorado should also consider adopting certain provisions from California's Information Practices Act.[187] The Information Practices Act protects the data rights of individual citizens by ensuring that state agencies use data only when appropriate.[188] Specific provisions that could be useful in protecting sensitive information from being given to HIEs are found in sections 1798.14 and 1798.15. Together, these sections provide a much-needed barrier between the nonvoluntary dissemination of private information and state agencies. Section 1798.14 provides that an agency will maintain "in its records only personal information which is relevant and necessary to accomplish a purpose of the agency."[189] Section 1798.15, on the other hand, requires agencies to collect personal information to the greatest extent practicable from the "individual who is the subject of the information rather than from another source."[190] These provisions guard against disclosure of private information by state agencies, which in turn affords citizens a higher level of protection in circumstances where government aid is being given through the state rather than the federal government.[191]

Finally, Colorado should reconsider its stance on the false light claim under the invasion of privacy torts. False light claims allow an individual to bring an action when incorrect information is distributed about her, but the distribution doesn't necessarily lead to a reputational injury. Just as an invasion of privacy claim for disclosure of private information rarely succeeds, a libel claim is similarly difficult to win because the reputation of a homeless individual may already be questionable. Thus, the claim for false light becomes useful. The Colorado Supreme Court previously maintained that most claims brought under a false light theory can be couched in an invasion of privacy claim for public disclosure of private affairs or a

---

beyond the scope of this Comment. For more information on the impact of socioeconomics on the ability to bring suit, see Stephen B. Bright, *Legal Representation for the Poor: Can Society Afford This Much Injustice?*, 75 MO. L. REV. 683 (2010).

187. CAL. CIV. CODE §§ 1798.78 (West 2019).

188. *See id.*

189. *Id.* § 1798.14.

190. *Id.*; *id.* § 1798.15.

191. *Id.* § 1798.14.

libel claim.[192] However, a claim for disseminating private information does not protect the same type of information as a claim for false light.[193] A claim for false light prevents untrue information from spreading, similar to defamation and libel, but it does not require injury to the plaintiff's reputation.[194] Whereas the claim for defamation is narrow and requires reputational injury, false light claims focus on the simple fact that disseminating untrue information leads to an emotional injury.[195] Thus, if Colorado were to recognize false light claims, it would protect an individual's interest in preventing the spread of false information.

D. A Band-Aid Fix

Another option is for Congress to give patients a choice of whether they want their EHR to be visible at all. A draft bill proposed by the Ministry of Health in Singapore gives patients the option of blocking access to their medical records on the national EHR.[196] If a patient chooses to block her information from providers in the national EHR, she is advised of the risks, "including in emergency situations, as healthcare providers will not be able to access [her] past healthcare information."[197] However, although providers cannot access the information, the patient's information is still uploaded to the national EHR so that if she decides to unlock the information in the future,

---

192. Denver Publ'g Co. v. Bueno, 54 P.3d 893, 903 (Colo. 2002). The court here also cited sensitivity to the fact that this tort can have First Amendment free speech implications. *Id.*

193. Laura A. Heymann, *The Law of Reputation and the Interest of the Audience*, 52 B.C. L. REV. 1341, 1411–12 (2012); RESTATEMENT (SECOND) OF TORTS § 652E(b) (AM. LAW INST. 1977). A false light claim includes where "the actor had knowledge of . . . *the falsity* of the publicized matter." *Id.* (emphasis added).

194. Heymann, *supra* note 193, at 1411–12.

195. Crump v. Beckley Newspapers, 320 S.E.2d 70, 87 (W. Va. 1983) (quoting Goodrich v. Waterbury Republican-American, Inc., 448 A.2d 1317, 1329 n.19 (Conn. 1982)).

196. *Public Consultation on Draft Healthcare Services Bill*, MINISTRY OF HEALTH SING., https://www.moh.gov.sg/docs/librariesprovider8/default-document-library/public-consultation-paper-on-draft-hcs-bill_171229933f1f50fd9d4ffcacde39d41e58f7db.pdf (last visited Jan. 18, 2019) [https://perma.cc/G6ET-MQML] (relevant language at § H-21; draft bill on file with author); Salma Khalik, *Draft Bill Eases Privacy Fears over Electronic Health Records*, STRAITS TIMES (Jan. 6, 2018, 5:00 AM), http://www.straitstimes.com/singapore/health/draft-bill-eases-privacy-fears-over-electronic-health-records [https://perma.cc/4NXM-TBA5].

197. *Public Consultation on Draft Healthcare Services Bill*, *supra* note 196.

all of the past data is accessible.[198] Similar to the United States' vision of a nationwide HIE system of EHR, the Singaporean national EHR is a universal system that "receives, consolidates, and maintains patient health records across different healthcare providers."[199]

If the concern is that SDH information is improperly processed for secondary uses outside the scope of the original consent, and the United States is not prepared to mitigate that concern via privacy laws, perhaps giving people the option of blocking access completely is the easiest way to achieve privacy. This Comment labels this a "Band-Aid fix" because, while it protects the privacy interests of the patient, only fixed legislation or rulemaking can appropriately consider the benefits of having SDH information available to healthcare providers while respecting the potential for privacy harms when data is improperly processed or used.

CONCLUSION

The United States has put immense amounts of time and effort into enhancing the healthcare system for the benefit of the patient. Laws that promote the use of EHR and HIEs are designed to enhance quality of care and lower overall healthcare costs. Laws and regulations that promote the use of valuable SDH information can help coordinate care to increase the efficacy of social programs. However, in the rush of technological change and influence of broad policy objectives, lawmakers have failed to consider how sensitive and private much of this information is. Individuals, especially those in difficult life situations, are struggling with issues that can impact their sense of social acceptance, security, and personhood.

As the United States moves toward fulfilling its vision of nationwide interoperability, lawmakers should put protections in place that balance the value of the fluid transmission of data with the privacy interests of the people whose data is being transmitted.

---

198. *Id.*

199. Yodi Hailemariam, *Singapore Addresses Confidentiality of Electronic Patient Records in New Healthcare Services Bill*, DRINKERBIDDLE (Jan. 24, 2018), http://dbrondata.com/2018/singapore-addresses-confidentiality-electronic-patient-records-new-healthcare-services-bill/ [https://perma.cc/P5BV-EJ9C]; *Meaningful Use*, *supra* note 19.

Ultimately, the United States should enact overarching federal data privacy protections for its citizens modeled, at least in part, on the current privacy laws in the EU.[200] Alternatively, sector-specific legislation or rulemaking could put an additional barrier, such as a privacy proxy, between SDH information and healthcare providers. While federal law is being created, states should protect their citizens by adopting laws similar to California's medical privacy laws and "Shine the Light" law.[201] Although state law is not as effective as overarching federal regulation for a scheme as large as an HIE, this would be an adequate gap-filler until Congress is able to reach a consensus on just what information should be protected.

200. COBB, *supra* note 152, at 3; Moneteiro, *supra* note 156; Eur. Council, *supra* note 157; Rotenberg & Jacobs, *supra* note 158; *Protection of Personal Data*, *supra* note 156.

201. McGuinness & Weis, *supra* note 16; Geroe & Biancamano, *supra* note 16.