GRANULAR CONTROL OF EHRS TO OVERCOME FRAGMENTED DISCLOSURE LAW: HOW POLICY CHOICES FOR GRANULARITY WILL AFFECT CLINICAL CARE, IMPACT SECONDARY USE OF HEALTH INFORMATION, AND ALTER RISKS FOR PATIENTS AND PROVIDERS

Katherine Drabiak-Syed, JD*

---

* Drabiak-Syed is a Law and Bioethics Policy Consultant to the Indiana University Center for Bioethics. This publication was supported by a grant from the Lilly Endowment to the Center for Law, Ethics & Applied Research in Health Information. Its contents are solely the responsibility of the author and do not reflect the official views of the Indiana University Center for Bioethics or the Center for Law, Ethics & Applied Research in Health Information.

I. INTRODUCTION

Effective utilization of electronic health records (EHRs) offers many promises to both clinicians and patients in the clinical care setting. Defined as a "repository of electronically maintained information about an individual's lifetime health status and health care," an EHR is longitudinal, comprehensive, and interoperable.[1] A full EHR contains a vast amount of a patient's clinical information designed to reduce errors, improve patient care, facilitate clinical coordination, and monitor care quality.[2] The information contained in an EHR gives providers a comprehensive reference of the patient's full medical history so providers may make more efficient and informed decisions during the course of care such as whether to order a test of procedure, whether a particular medication would counteract with any of the patient's current medications or drug allergies, and cross reference relevant information in the patient's medical history. [3] The aggregate information and its availability to providers decrease the number of tests to which the patient is subjected and lowers the risk of potentially problematic drug responses.[4] EHR systems also offer the potential to provide clinical decision support to physicians by checking patient medication interactions,

---

[1] Sharona Hoffman & Andy Podgurski, *E-Health Hazards: Provider Liability and Electronic Health Record Systems*, 24 Berkeley Tech. L.J. 1523, 1530 (2009); Mark Rothstein, *The Hippocratic Bargain and Health Information Technology*, 38 J.L. Med. & Ethics 7, 9 (2010) [hereinafter Rothstein, *E-Health Hazards*].

[2] Leslie Pickering Francis, *The Effects of Health Information Technology on the Physician-Patient Relationship: The Physician-Patient Relationship and a National Health Information Network*, 38 J.L. Med. & Ethics 36 (2010).

[3] MELISSA GOLDSTEIN & ALISON REIN, CONSUMER CONSENT OPTIONS FOR ELECTRONIC HEALTH INFORMATION EXCHANGE: POLICY CONSIDERATIONS AND ANALYSIS, 2, 61 (2010), *available at* http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy_and_security/1147.

[4] *Id.* at 61; Elana Rivkin-Haas, Note, *Electronic Medical Records and the Challenge to Privacy: How the US and Canada are Responding*, 34 HASTINGS INT'L & COMP. L. REV. 177 (2011).

providing test recommendations, or offering suggestions for treatment options based on best practices guidelines.[5]

Adoption of EHRs will offer significant savings to health care providers and reduce costs in the healthcare system. The American Recovery and Reinvestment Act of 2009 (ARRA) invested $19 billion in computerized medical records in an effort to eventually reduce medical care costs while increasing effective patient care and protecting patient privacy.[6] The Health Information Technology for Economic and Clinical Care Act (HITECH Act) encourages health care providers and physicians to adopt an EHR system before 2015 and contains funding incentives for EHR infrastructure and technology implementation.[7] Provider access to information contained in an EHR can eliminate costly inefficiencies, such as ordering redundant testing and diagnostic services, and the use of clinical decision support features allow providers to quickly identify illnesses and mitigate the potential for medical errors.[8] As providers begin to utilize EHRs, evidence suggests that provider access to patient's complete records along with EHR clinical guidance will reduce costs by $142-371 billion annually.[9]

States that have taken the initiative and begun to build their health information exchanges (HIEs) face a number of regulatory and legal barriers to the implementation of policies and procedures governing the collection, disclosure, and use patients' medical information. Health information organizations (HIOs) are faced with a fragmented architecture of federal and state law where many states permit the collection of general patient information to enter

---

5 Jonathon Roth, Note, *Regulating Your Medical History Without Regulations: a Private Regulatory Framework to Electronic Health Record Adoption*, 91 B.U.L. Rev. 2103, 2106-2109 (2011).

6 Stephen Weiser, *Breaking Down the Federal and State Barriers Preventing the Implementation of Accurate, Reliable, and Cost Effective Electronic Health Records*, 19 ANNALS HEALTH L. 205, 205-06 (2010).

7 *Id.* at 206.

8 Roth, *supra* note 5, at 2108-2109.

9 John Hill et al., *A Proposed National Health Information Network Architecture and Complementary Federal Preemption of State Health Information Privacy Laws*, 48 AM. BUS. L.J. 503, 509 (2011).

in an HIE without additional patient consent, but some states contain additional provisions restricting the disclosure of sensitive medical information without additional patient consent, posing functional and operational uncertainties. These legal questions have prompted HIOs and policymakers to discuss whether to include sensitive information in the HIE or whether to implement a system of granular control for sensitive patient information. Each option and permutation related to the HIO's treatment of sensitive information corresponds to differences in clinical care, the ability to use the data in the HIE for research purposes, and potential provider liability in the clinical care setting.

As more healthcare systems begin to adopt EHR technology and states continue building their health information organizations (HIOs) to manage EHRs, the sheer amount of patient information in health information exchanges (HIEs) and its utility and accessibility increases. Digitalization of data and physician-patient interactions facilitates the ability to collect, store, replicate, and transmit information contained in the EHR by authorized persons involved in clinical care.[10] In addition to clinical use of EHRs, HIEs offer great promise to public health officials and investigators who can use the information contained in EHRs for purposes such as quality assessment, public health reporting, and research to eventually return these findings into more efficient and effective clinical care.[11] However, increasing the amount of persons who may have access corresponds to a higher potential for improper disclosures of patients' private medical information.[12] Furthermore, options for granularity means that physicians will not have access to patients' complete records, which may impair physician's ability to appropriately treat patients according to evolving standards of care and expose physicians to a new area of liability.

Part I of this article contains an overview of federal and state laws relating to the collection, use, and disclosure of

---

10 GOLDSTEIN, *supra* note 3, at 53.

11 *Id.* at 24-25.

12 *Id.* at 52.

protected health information (PHI) and two subsets of sensitive health information, specifically mental health records and substance abuse and treatment records. This portion of the article discusses the barriers to interstate interoperability and secondary uses of data in HIEs arising from varied state law approaches governing the disclosure of these records. Part II provides an overview of the policy movement toward granular control of sensitive information and corresponding considerations for clinical care. Part III discusses three HIOs and associated state law in Indiana, New York, and Arizona, which have each adopted varied methods of building an HIO. This portion of the article outlines how these models answer the policy questions related to how patients participate in the HIE, how the state approaches treatment of sensitive information, and potential tradeoffs to patient privacy, clinical care, and research associated with each policy choice. The next portion of the article examines long term issues connected to amassing patient information in HIEs and assesses specific considerations based on how the HIE approaches integrating sensitive information. Part IV discusses how the data in the HIEs could be used for public health and research purposes designed to return clinical care benefits to patients and highlights the synergy between respecting patient privacy and the ability to derive public health information. Next, Part V notes the growing potential for wrongful disclosures and security breaches of health information and asserts that the information contained in HIEs may become a target for wrongdoing, which increases the risk that patients may suffer adverse consequences that affect not only their finances and insurance, but also their future clinical interactions. Lastly, Part VI predicts how systems of granularity will affect a physician's ability to treat patients. HIEs that fully sequester sensitive information or keep sensitive information hidden in the HIE may impair the physician's ability to effectively treat patients and correspond to an increase in provider liability and medical malpractice actions.

II. DISCLOSURES OF HEALTH INFORMATION

States and HIOs building or expanding their HIEs must navigate federal and state law, which is both complex and quickly evolving. Federal law and regulations set forth standards governing the uses of protected health information (PHI), requirements for disclosing and sharing PHI and security standards to safeguard the information.[13] State law expands and complements the federal floor for protecting the privacy of health information, setting forth additional requirements governing uses and disclosure of general medical information, and some states set forth distinct requirements for categories of sensitive medical information.

A. Federal Law

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule governs the uses and disclosures of PHI, such as names, medical record numbers, social security numbers, and medical record information by covered entities including health care providers and health plans.[14] Under the Privacy Rule, covered entities may not use or disclose PHI without an authorization unless otherwise permitted or required by law.[15] Covered entities may use and disclose PHI without an authorization for uses such as treatment, payment, and healthcare operations, and use a limited data set without an individual's authorization for research purposes and public health operations, and may always use or disclose for individual health information which has been de-identified.[16] If a covered entity wishes to disclose and use PHI for additional purposes not otherwise permitted, required, or exempted, the covered entity must obtain an authorization from the patient specifying how the PHI will be used or disclosed, to whom the information will

---

13 See GOLDSTEIN, *supra* note 3, at 40-42.

14 45 C.F.R. § 160.103 (2011); *see* GOLDSTEIN, *supra* note 3, at 42-44.

15 45 C.F.R. § 164.502(a) (2011).

16 45 C.F.R. § 164.506 (2011).

be disclosed, and the length of time the authorization is valid.[17]

The HIPAA Security Rule sets forth standards designed to protect the confidentiality and integrity of the information maintained, used, and transmitted by covered entities.[18] Under the Security Rule, covered entities must implement reasonable administrative, physical, and technical safeguards to secure electronic health information.[19] It provides specific technological guidelines designed to increase data security such as creating log-in systems accessible by password, using encryption programs, and auditing data access.[20]

In 2009, Congress passed the Health Information Technology for Economic and Clinical Care Act (HITECH Act), which is designed to advance the use of health technology by funding incentives for healthcare providers to adopt an EHR system by 2015.[21] Importantly, the HITECH Act also set forth a second priority to use electronic health data to enhance the use of health information technology in healthcare through population health research and clinical research.[22]

As states continue to build their HIOs, they face differing requirements for Privacy Rule compliance based on their functional purpose.[23] If a covered entity enters

---

17 45 C.F.R. § 164.508 (2011).

18 Martha Tucker Ayres, *Confidentiality and Disclosure of Health Information in Arkansas*, 64 ARK. L. REV. 969, 983 (2011).

19 45 C.F.R. § 164.302 (2011); 45 C.F.R. § 164.304 (2011); 45 C.F.R. § 164.306 (2011).

20 45 C.F.R. § 164.308; Ayres, *supra* note 18, at 983.

21 Weiser, *supra* note 6, at 206.

22 *Id.*

23 *See* Kari Bomash, *Privacy and Public Health in the Information Age: Electronic Health Records and the Minnesota Health Records Act*, 10 MINN. J.L. SCI. & TECH. 117, 121-122 (2009) (discussing using EHRs for public health purposes); *See* Kenneth Goodman, *Ethics, Information Technology, and Public Health, New Challenges for the Physician-Patient Relationship*, 38 J.L. MED. & ETHICS 58, 59-62 (2010) (discussing using EHRs for surveillance programs and community health programs; *See* Pickering Francis, *supra* note 2, at 43-45 (discussing using EHRs to improve patient care and patient choices);

patient information into a health information exchange (HIE) to facilitate health care treatment and operations, the law as written does not require patients to authorize entry of their PHI.[24] However, if the health information organization (HIO) adopts the HITECH Act's second priority to use the health data for research purposes, then the HIO may need patient authorization to use or disclose PHI for particular research uses where the patient is identifiable.[25] An HIO's future use of patient information poses at least one dilemma and becomes further complicated by vastly different state laws protecting the use and disclosure of types of health information that the HIO may use or exchange for secondary purposes. Currently, the use of EHRs is fragmented and disconnected, posing a confusing architecture of health records and creating dizzying permutations: whether a state contains an HIO, which providers transmit information to that HIO, whether the HIO uses or contemplates using the information for secondary purposes, and whether the HIO contains records from a singular state or exchanges records from multiple states.

Although the Office of the National Coordinator for Health Information Technology promulgates a goal of EHR interconnectivity, the ARRA does not require federally funded systems to be functionally interoperable but rather requires that "interconnection be possible."[26] The goal of future intrastate and interstate interoperability along with varying HIO agendas and state law relating to disclosure requirements poses additional challenges for HIEs because providers and HIOs must understand the requirements set forth in federal law, the law of the operating state, and the law to where the information may be exchanged for clinical care or secondary purposes.[27] That is, information gathered

---

See Pickering Francis, supra note 2, at 45 (discussing using EHRs for quality improvement purposes).

[24] *See* GOLDSTEIN, *supra* note 3, at 42-44

[25] 45 C.F.R. § 164.508.

[26] Mark A. Hall, *Property, Privacy, and the Pursuit of Interconnected Electronic Medical Records*, 95 IOWA L. REV. 631, 635 (2010).

[27] Hill et al., *supra* note 9, at 531-532.

for clinical care purposes and entered into the state's HIE may travel to another state that contains differing restrictions on the disclosure of specific subsets of information and varying standards on how that information may be used without further authorization from the original patient.

B. State Law

HIPAA's requirements establish a floor of protection for use and disclosure of individually identifiable information, which provides each state the ability to enact more stringent laws relating to general medical records or subsets of records that include sensitive categories of information.[28] States vary with regard to how they define terms such as medical record or medical information, to whom this information can be disclosed, for what purposes, what an individual's consent to disclose this information must contain, and the nature of exceptions for disclosure without consent.[29] As more states begin to build their HIOs, the question arises whether entering patient information into a record locator system and physician access to that information constitutes separate additional disclosures or whether they are implicitly permitted disclosures that do not require additional patient consent. In addition to general medical information, some states set forth additional protections to guard the confidentiality of sensitive medical information. These states may require additional consent from patients to include types of sensitive records in the HIE and limit subsequent disclosures of these records from the HIE. This extensive disparity among states relating to defining permissible disclosures also poses questions of how to resolve these discrepancies and what model of interstate choice of law or preemption should govern during the interstate exchange of

---

[28] *See* Goldstein & Rein *supra* note 3, at 40-42.

[29] JOY PRITTS, ET AL., PRIVACY AND SECURITY SOLUTIONS FOR INTEROPERABLE HEALTH EXCHANGE: REPORT OF STATE MEDICAL RECORD ACCESS LAWS, at 3-2 (2009), http://www.healthit.gov/sites/default/files/290-05-0015-state-law-access-report-1.pdf.

information.[30] Furthermore, some state laws carve out exceptions for disclosure restrictions to use medical information (sometimes inclusive of sensitive information) for research purposes, which poses several choice of law questions if the HIO exchanges this information with other states.

1. Health/Medical Information and Records

Based on HIPAA's standard, most states have adopted a model where a patient does not need to provide the treating physician authorization to use the patient's current medical record for treatment purposes and permits additional disclosure of medical information to directly consulting providers or excludes this transfer from the definition of disclosure.[31] Many states specify that patient health care or medical records are confidential and place limitations on their disclosure for secondary purposes. Some states permit the release of health or medical records for general research purposes, public health research, or scientific, medical, or public policy research.[32] The states that permit the disclosure of these records contain corresponding provisions designed to protect the confidentiality of the patients through various methods such as specifying that the researcher shall maintain the confidentiality of the records,

---

[30] Hill et al., *supra* note 9, at 531-32.

[31] New York is one exception that requires patient consent for treatment, payment and healthcare operations. *See* N.Y. COMP. CODES R. & REGS. tit. 10, § 405.10(a)(6) (2012); N.Y. EDUC. LAW § 6530(23) (McKinney 2012); N.Y. COMP. CODES R. & REGS. tit. 8, § 29 (2012).

[32] *See* CAL. CIV. CODE § 56.10(c)(7) (West 2012) (noting that the disclosure of health/genetic information is permitted for certain research where the identity of patient protected); COLO. REV. STAT. ANN. § 6-18-103 (repealed 2004) (discussing permissible releases of health information for research purposes, including genetic information, so long as the identity of the individual is not disclosed); 410 ILL. COMP. STAT. ANN. 520/5 (West 2012) (discussing a confidentiality provision in state public health law that outlines conditions and procedures specified for outside research); NEB. REV. STAT. ANN. § 44-916(2) (West 2012) (permitting disclosures without the authorization of the individual for the performance of several activities, including "scientific, medical or public policy research.")

the researcher must protect the patient identities, or the researcher may not disclose patient identities to external entities not involved in the research or must provide written assurances of confidentiality[33] A minority of states allow health care providers to release health and medical records containing the patient's identifying information without the patient's authorization for research if an IRB approves the research project[34] or the IRB determines the project satisfies a list of criteria.[35]

As HIOs collect patient information and implement a record locator system (RLS), some privacy advocates have argued that entry of patient information into the HIE and even patient listing in the RLS requires patient consent because these are additional disclosures outside the traditional one-to-one treatment relationship between physician and patient.[36] The ONC Tiger Team recommends that directed exchange of medical information solely for treatment does not require consent unless otherwise specified in law or custom.[37] However, privacy activist

---

[33] *See* UTAH CODE ANN. § 26-33a-109 (West 2012) (discussing how the collection of permitted health data must be kept confidential and a written agreement to protect data is required); Cal. Civ. Code §56.10(c)(7) (West 2012) (noting that the disclosure of health/genetic information is permitted for certain research where the identity of patient protected); COLO. REV. STAT. ANN. § 6-18-103 (2003) (discussing permissible releases of health information for research purposes, including genetic information, so long as the identity of the individual is not disclosed) (repealed 2004); WIS. STAT. ANN. § 146.82 (West 2012) (discussing how the release of medical information for research permitted where identity of subject is protected).

[34] N.D. CENT. CODE ANN. § 23-01.3-02 (West 2012) (use of biomedical health information is permitted for research approved by an IRB or for public health research where identity of patient is protected).

[35] WASH. REV. CODE ANN. § 70.02.050 (West 2012) (stating that disclosure without patient authorization is permitted for research approved by an institutional review board that has met certain criteria).

[36] DEBORAH PEEL, WRITTEN TESTIMONY BEFORE THE HIT POLICY COMMITTEE (Sept. 18, 2009) [hereinafter PEEL, WRITTEN TESTIMONY], http://epic.org/privacy/medical/Peel_PPR%20Written%20testimony%20HIT%20Policy%20Committee.pdf.

[37] PAUL TANG, RECOMMENDATIONS FROM THE PRIVACY & SECURITY TIGER TEAM TO THE HIT POLICY COMMITTEE, 9 (Sept. 1, 2010) [hereinafter HIT POLICY COMMITTEE LETTER], http://healthit.

Deborah Peel argues that EHR systems are fundamentally different than paper records because of higher privacy and security risks, and maintains that providers should obtain consent to access patient information in an HIE.[38] In New York, the New York Civil Liberties Union has argued that state law requires patient consent at two points: (1) to add patient information into the RLS and HIE, and (2) when a physician seeks access to patient information in the HIE.[39] The potential points of consent-entry into the RLS, consent for provider access, or consent for secondary uses of the information pose a potentially confusing situation for HIOs exchanging information that have differing policies regarding what action constitutes a disclosure and when the patient must consent. Furthermore, HIOs operating in states without research provisions that wish to utilize the exchange only for clinical care purposes but exchange records across states would need to establish a method of segregating medical records from being used in other states for secondary purposes after the initial clinical care disclosure.

2. Sensitive Records

Many states provide additional statutory provisions governing the privacy and disclosure of subsets of sensitive health information such as mental health records, substance abuse treatment records, genetic information, health records relating to domestic violence, or reproductive

---

hhs.gov/portal/server.pt/gateway/PTARGS_0_0_6011_1815_17825_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/ files/hitpc_transmittal_p_s_tt_9_1_10.pdf.

[38] Deborah Peel, *Your Medical Records Aren't Secure*, WALL ST. J. (Mar 23, 2010) [hereinafter Peel, *Your Medical Records Aren't Secure*], *available at* http://online.wsj.com/article/SB10001424052748703580904575132111888664060.html.

[39] Corrine Carrey & Gillian Stern, *Protecting Patient Privacy: Strategies for Regulating Electronic Health Records Exchange*, NEW YORK CIVIL LIBERTIES UNION (Mar. 2012), *available at* http://www.nyclu.org/files/publications/nyclu_PatientPrivacy.pdf; *see also* Bomash, at 127 (2009) (discussing patient consent to enter information into the RLS).

care information.[40] In general, some states contain provisions stating that a particular type of record is confidential and the patient must explicitly consent to its disclosure.[41] States differ with regard to what types of information its statutes afford additional protection, whether it affords additional protection for one or several subsets of information, and the scope of exceptions to the disclosure provisions. Many states that restrict the disclosure of sensitive information provide disclosure restriction exceptions for public health purposes, research purposes, as well as exceptions where required by law, such as for reporting purposes.[42] Navigating the variation among state law's additional disclosure requirements has prompted federal guidance from the ONC's Tiger Team and scholars recommending that providers sequester sensitive information and separate it from the rest of the patient record or provide granular control over these subsets of medical information.[43]

In general, drug and alcohol records including patient identifying information that are maintained in connection with the performance of any substance abuse treatment or prevention program are confidential and require patient consent to release these records. Under the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act, federal law places limitations on

---

[40] *See* 42 C.F.R. § 59.11 (2012) (confidentiality for patients receiving federally funded family planning services); PRITTS, *supra* note 29, at 3-15 to 3-18; GOLDSTEIN, *supra* note 3, at 48 (discussing the federal and state requirements for substance abuse and treatment records).

[41] See for example New York, who provides additional protections for disclosing genetic information, N.Y. CIV. R. LAW §79-l (McKinney 2012), mental health information, N.Y. MENTAL HYG. LAW § 33.13 (McKinney 2012), and substance abuse and treatment information, N.Y. PUB. HEALTH LAW §§ 3371, 3372 (McKinney 2012).

[42] ARK. CODE ANN. § 20-09-304 (West 2012) (providing that medical information may be released for research where identity of patient protected).

[43] Rothstein, *E-Health Hazards*, *supra* note 1, at 11-12; *see also* HIT POLICY COMMITTEE LETTER, *supra* note 37 (providing recommendations to HHS on privacy and security policies and practices);

disclosures of patient information for individuals in drug or alcohol abuse treatment programs that receive federal funding, and some states provide additional limitations on disclosure of substance abuse records.[44] Some state laws explicitly require that during treatment, providers must uphold the confidentiality of patient information and not disclose such information to external parties to preserve the confidences of the patient.[45] Several states contain provisions that allow disclosure of this information from non-federally funded programs including the patient's identifying information without the patient's authorization or consent for specific purposes, such as releasing the records to qualified personnel for the purpose of conducting scientific research,[46] or releasing the records for research into the causes and treatment of drug and alcohol abuse.[47] Some states place additional restrictions on this disclosure of records and specify that the records may not identify the patient or contain identifying information,[48] while states such as Maine allow the researcher access to the identifying information as long as this information is not published.[49]

Mental health records including patient identifying information that are maintained in connection with the performance of evaluation and treatment programs are confidential and states generally limit disclosures of this

---

[44] *See* 42 C.F.R. § 2.3(a) (2011).

[45] *Supra* note 32.

[46] *See* CAL. HEALTH & SAFETY CODE § 11845.5 (West 2012) (stating that the disclosure of substance abuse records permitted for research if patient cannot be identified); *see also* CAL. HEALTH & SAFETY CODE § 11977 (2003) (repealed 2004).

[47] *See* S.D. CODIFIED LAWS § 34-20A-91 (2011) (repealed 2012) (the release of records from alcohol and drug treatment permitted for research where patient identifying information not disclosed).

[48] *See* CAL. HEALTH & SAFETY CODE § 11845.5 (West 2012) (the disclosure of substance abuse records permitted for research if patient cannot be identified); MICH. COMP. LAWS ANN. § 333.6113 (West 2012) (using substance abuse records for research where identity of patient not disclosed).

[49] *See* ME. REV. STAT. ANN. tit. 5, § 20047 (West 2012) (stating that the registrations and other records of treatment facilities for substance abuse should remain confidential although the information may be released for research purposes).

information. Similar to substance abuse and treatment records, state law and professional guidelines maintain that during treatment providers must uphold the confidentiality of patient information and not disclose such information to external parties.[50] The American Medical Association's Code of Medical Ethics and the American Psychological Association's Ethical Principles of Psychologists and Code of Conduct each set forth a professional obligation to protect a patient's confidential information learned during treatment, noted the importance of confidentiality in patient trust and effective care, and discussed limitations on disclosure.[51] Some state laws permit research use of mental health records, and most of those states contain provisions designed to protect the identity of the patients by specifying that the researcher must keep the identities of the clients confidential and may not further disclose any identifying information[52] or must provide assurances that the anonymity of the patient will be protected (Alaska).[53] States differ with regard to who may access and use these records and identifying information, ranging from only the state Secretary of Health or designee (Florida), to qualified personnel (District of Columbia), to a person doing research or conducting health statistics as part of a bona fide research program (Alaska).[54]

---

[50] *Patient Confidentiality*, AMERICAN MEDICAL ASSOCIATION, *available at* http://www.ama-assn.org/ama/pub/physician-resources/legal-topics/patient-physician-relationship-topics/patient-confidentiality.page (last visited Nov. 4, 2012); *Ethical Principles of Psychologists and Code of Conduct*, AMERICAN PSYCHOLOGICAL ASSOCIATION, *available at* http://www.apa.org/ethics/code/ index.aspx (last visited Nov. 4, 2012).

[51] *Id.*

[52] *See* D.C. CODE § 7-242 (2010) (amended 2012) (describing the permissible uses and disclosures of health information, including certain types of research); D.C. CODE § 7-1203.05 (West 2012) (providing a research exception to general rule of confidentiality of health info about mental health patients); FLA. STAT. ANN. § 394.4615 West (2012) (permits disclosure of mental health records for research purposes).

[53] ALASKA STAT. ANN. § 47.30.845(4) (2012) (stating that the disclosure of mental health data to a researcher is permitted when anonymity of the patient assured).

[54] *Id.*

When an HIO develops its policies relating to sensitive patient information, it would need to understand a significant amount of legal, policy and procedural information: what type or types of sensitive records are involved; whether the content of the records will be used solely for clinical care or held in the HIE for potential research; state law where the initial treatment occurred relating to disclosing sensitive information for clinical care, to an HIO, and for secondary purposes; law of the destination state relating to disclosing sensitive information for clinical care, to an HIO, and for secondary purposes. Improper information segmentation or confusing statutory preemption analysis could potentially lead to thorny scenarios where one state strictly limits the disclosures of sensitive information but exchanges this information to another state with vastly different laws. These questions have prompted policymakers and scholars to rethink whether and how to include or permit access to patients' sensitive information in HIEs and whether granular control of sensitive medical information constitutes a policy alternative.

III. GRANULARITY AND SENSITIVE MEDICAL INFORMATION

The Office of the National Coordinator for Health Information Technology's HIT Policy Committee has asserted that a form of granular control over health data can protect the confidentiality of narrow categories of sensitive health information while fostering patient autonomy, promoting trust in medical providers, and building confidence in the growing use of HIT.[55] Policymakers recognize that patients would like to exert some influence over who views this information and have discussed various systems of granular control over sensitive information.[56] Proposed mechanisms for asserting granular

---

[55] *Advancing Privacy and Security in Health Information Exchange*, HHS.GOV (Sept. 12, 2011), http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy_and_security/1147 (last visited Oct. 18, 2012) [hereinafter *Advancing Privacy*].

[56] Goldstein, *supra* note 3, at 7-10, 19 (discussing types of granularity by data type, provider, time range, or purpose).

control and increasing patient privacy vary, each solution with its own tradeoff to the provision of comprehensive and effective clinical care as well as implications for research. The New York Civil Liberties Union has taken the position that HIOs should sequester records and make them available to subsequent providers through the HIE only with specific patient consent at two points: prior to entering the information into the HIE and prior to the disclosure to the requesting physician.[57] Building upon this notion of controlling disclosures, Professor Pickering Francis has suggested that HIOs should instead include all patient information in the HIE, but mask and flag sensitive information, so providers are aware of its existence when they view the patient's full record and can request patient consent to view the entire record.[58]

Despite an increase in patient privacy, systems of granular control and mechanisms to exclude sensitive information from an HIE hold several drawbacks. Given the amount of different types of sensitive information and the methods to offer granular control over its access, patients may end up facing too many choices, resulting in confusion or exercise of meaningless choice.[59] Granular control of sensitive information may pose logistical feasibility setbacks for providers accommodating different patient choices and attempting to track disclosures of this information should the patient revoke authorization for release of the information.[60] Whether an HIO excludes sensitive information from its exchange or includes it in fully masked form, both scenarios carry highly problematic implications for clinical care.[61] The type of information involved in sensitive records can provide physicians crucial information to the patient's state of mind, whether the patient's decision-making capacity is influenced by external

---

[57] Carrey, *supra* note 39, at 16-17.

[58] Francis, *supra* note 2, at 40-42.

[59] Mark Rothstein, *Debate Over Patient Privacy Controls in Electronic Health Records*, BIOETHICS FORUM (February 17, 2011), http://www.thehastingscenter.org/Bioethicsforum/Post. aspx?id=5139.

[60] Weiser, *supra* note 6, at 210.

[61] *Id.* at 209-10.

factors (mental health struggles or substances), or whether the patient is taking or using any contraindicated drugs. This scenario results in a thorny dilemma; that is, a patient chooses to exclude or hide some subsets of information because of its sensitive nature, yet patients who have mental illness or struggle with substance abuse issues - both of which are often lifelong residual struggles - may be most in need of attentive and complete care.

Furthermore, sensitive information would be especially relevant to providing comprehensive care in an emergency situation, contrary to the New York Civil Liberties Union's assertion.[62] Both the pace of care and potential for life threatening conditions mean that missing a piece of sensitive information about the patient could conceal the patient's underlying condition. Imagine the following two patient scenarios: (1) Giving oxycodone to Patient A with an excruciating backache; and (2) respecting Patient B's religious request to refuse a life saving blood transfusion after an attempted suicide. However, imagine if the physician could have accessed sensitive records for these two patients to find that Patient A's excruciating pain arose from illegal substance abuse withdrawal and Patient B had a history of religious guilt, which fueled his depression and suicide attempts. If EHRs are designed to enhance clinical care and provide physicians the information necessary to make the most informed decisions, then sensitive information may be especially crucial in emergency situations.

IV. STATE HIO MODELS: INDIANA, NEW YORK, AND ARIZONA

Several states have worked to construct their EHR systems by varying methods such as building a statutory framework or promoting an HIO that promulgates policies aligned with current state law. [63] As states continue to expand or initiate their HIOs, they must consider: (1) current state law relating to disclosing medical information

---

[62] Carrey, *supra* note 35, at 15.

[63] *See* Goldstein, *supra* note 3 (discussing state HIOs in operation and models of consent).

and sensitive records; (2) how patients will participate in the HIE and the issue of consent; (3) at what points the HIO or provider will obtain consent; and (4) determining access to patient records in the HIE and whether the records will be used exclusively for clinical care or also for secondary purposes. The following section examines three models in Indiana, New York, and Arizona, assesses policy choices, and examines potential tradeoffs.

A. Indiana

Indiana state law sets forth details for the construction of a corporation to build and manage a statewide electronic health information exchange.[64] Indiana's statutory law is comprehensive, specifically addressing the duties of the corporation, its purpose, and directions for its operation. The Indiana legislature directed that the health information exchange should "improve the health of the citizens of Indiana" by designing and implementing both an exchange of clinical health information as well as planning and facilitating research activities.[65] Indiana resolves the question of whether the patient must consent for disclosures by classifying patient health records as the providers' property.[66] Under Indiana law, providers may use a patient's original health record without specific authorization for a number of "legitimate business purposes" including entering the patient record into the Indiana Health Information Exchange (IHIE) or disclosing to another provider, for "scientific, statistical, and educational purposes," or "data aggregation projects" by the Indiana hospital trade association.[67] The IHIE has incorporated the state's comprehensive statutory scheme to create a system that connects over ninety hospitals and healthcare providers throughout the state with a flow of

---

64 IND. CODE ANN. § 5-31-6-1 (repealed 2012).

65 IND. CODE ANN. §§ 5-31-6-1, 5-31-1-1, 5-31-6-2 (repealed 2012).

66 IND. CODE ANN. § 16-39-5-3 (West 2012).

67 *Id.*

health data. [68] State law relating to sensitive records follows two differing standards. State law defines mental health records as confidential and that notes that they generally may only be disclosed with consent, but references an exception that mental health records may be disclosed without consent for "legitimate business purposes," which as defined above, includes disclosure to the IHIE.[69] Indiana references and follows federal law for the disclosure of alcohol and drug abuse patient records.[70]

IHIE has generally been regarded as a positive model for initiating and building an HIE marked by efficiency and ever increasing expansion.[71] Indiana approaches each policy question by systematically addressing them by statute. However, Indiana law also provides for abolishment of the corporation in 2015, leaving operational questions open to IHIE and future legislation. Additionally, privacy advocates and legal scholars have criticized the concept of operational models that do not obtain patients' affirmative consent to use health information from an HIO for research purposes.[72] Privacy advocates may also take issue with the statutory allowance to disclose mental health information for research purposes without additional patient authorization.

B. New York

New York state law is scattered through various sections of code, does not address requirements or guidelines for a health information exchange directly, and contains

---

[68] *About IHIE*, INDIANA HEALTH INFORMATION EXCHANGE, http://www.ihie.org/About/ default.php (last visited Oct. 18, 2012).

[69] IND. CODE ANN. § 16-39-2-3 (West 2012).

[70] IND. CODE ANN. § 16-39-1-9 (West 2012).

[71] Deanna Porgorelc, *Lessons From a State at the Front Lines of Health Information Exchange*, MEDCITYNEWS.COM (April 6, 2012, 10:29 AM), http://medcitynews.com/2012/04/lessons-from-a-state-at-the-front-lines-of-health-information-exchange/.

[72] PEEL, WRITTEN TESTIMONY, *supra* note 36; *see also* Mark Rothstein, *Improve Privacy in Research by Eliminating Informed Consent? IOM Report Misses the Mark*, 37 J.L. MED. & ETHICS 507 (2009) [hereinafter Rothstein, *Improve Privacy*].

potentially ambiguous and confusing language.[73] One notable element in New York law is that unlike HIPAA and most other states, patients must provide consent to disclose their medical records even for treatment purposes (except in an emergency).[74] Founded in 2006, the New York eHealth Collaborative (NYeC) is the state's non-profit entity that has worked to develop policies and standards for health information exchange in the state and coordinate the creation of a network to connect state providers.[75] NYeC's focus has been on facilitating connection and continuity between the regional health information organizations (RHIOs) in the state for clinical care, although state statute and NYeC policies do discuss using de-identified data for research purposes.[76] In an effort to clarify state law and set forth policy stances, the NYeC has issued recommendations for consumer consent policies in addition to outlining comprehensive operational standards.[77] NYeC policy instructs participating providers to enter patient information into the RLS and exchange, and subsequent providers must obtain consent from patients to access the information.[78] Under NYeC policy and state law, providers may choose whether to enter sensitive information as permitted by law into the exchange and providers may

---

[73] *See New York Health Information Exchange Operational Plan,* NYEHEALTH.ORG, at 72-75 (Oct. 26, 2010), http://nyehealth.org/images/files/File_Repository16/pdf/nys_hie_operational_plan_2010.pdf [hereinafter *New York Health*].

[74] N.Y. COMP. CODES R. & REGS. TIT. 10, § 405.10(a)(6) (2012); *see Recommendations for Standardized Consumer Consent Policies and Procedures for RHIOs in New York to Advance Interoperable Health Information Exchange to Improve Care,* NEW YORK EHEALTH COLLABORATIVE 1, 73 (Nov. 2008), http://nyehealth.org/images/files/File_Repository16/pdf/Consent_White_Paper_ 20081125.pdf [hereinafter *Consumer Consent Policies*].

[75] *About Us,* NEW YORK EHEALTH COLLABORATIVE, http://nyehealth.org/about-nyec/ (last visited Nov. 5, 2012).

[76] *Consumer Consent Policies, supra* note 74, at 24.

[77] *Id.*; *New York Health, supra* note 73.

[78] *See Consumer Consent Policies, supra* note 74, at 22-23 (noting that one-to-one direct exchanges are not subject to standard paper consent requirements); *see also* N.Y. PUB. HEALTH LAW § 18(1)(e) (2012); N.Y. PUB. HEALTH LAW § 18(6) (2012).

access the information through the exchange by obtaining patient consent.[79]

In March 2012, the New York Civil Liberties Union published a position paper criticizing perceived legal and policy shortcomings of NYeC's operational policies.[80] NYCLU challenged NYeC's interpretation of state law relating to consent, arguing that initial inclusion of patient information in the exchange also requires consent. Although physicians must obtain consent to view patient information in the exchange, participating providers enter patient medical information into the exchange without patient consent and patients cannot opt-out of the RLS. Furthermore, NYeC's comprehensive records means there is no formal mechanism for patients to limit sharing stigmatizing sensitive information such as substance abuse records or mental health treatment if they participate in the exchange. In April 2012, the New York Department of Health and the New York eHealth Collaborative established the State Health Information Network of New York Policy Committee to examine these and numerous other concerns over the state's current policies and procedures governing the exchange.[81]

C. Arizona

Sparked by gubernatorial order in 2005, Arizona has been working to develop the state's HIO through legislation and partnership with the Arizona Health-e Connection (AHeC). Arizona has passed comprehensive legislation directly addressing policies and procedures for a working HIO in the state, taking note of recent policy discussions relating to consent and granular control options for sensitive information. AHeC is a public-private partnership working to facilitate the design and implementation of a

---

[79] *See Consumer Consent Policies*, *supra* note 74, at 21, 28; *New York Health*, *supra* note 73, at 73; N.Y. MENTAL HYG. LAW § 33.13.

[80] Carrey, *supra* note 39.

[81] Nicole Lewis, *New York Moves to Protect Health Data Privacy*, INFORMATIONWEEK.COM (April 5, 2012), http://www.informationweek.com/news/healthcare/security-privacy/232800368.

statewide HIE, which is still in its initial stages.[82] Arizona state law sets forth a specific statutory scheme for the HIO's governance and policy operations.[83] Under Arizona law, the HIO must provide notice to patients to inform them that it collects individually identifiable health information, who may have access to this information, for what purposes, and how the patient may opt-out of the HIE.[84] Participating providers will enter patients' information into the exchange and patients have the opportunity to opt-out.[85] Patients may also choose to partially opt-out by requesting that a particular provider withhold its patient information from the HIE.[86] State law mandates that the HIO must implement a technologically functional system for segregating or sharing health information by 2015.[87] The HIO may disclose the individual's identifiable health information as long as the disclosure comports with HIPAA, but may not transfer individually identifiable or deidentified information for research unless the patient provides consent.[88]

Arizona's extensive and specific legislation incorporates recent policy discussions relating to promoting patient education about HIOs and providing patients with options for granular control of sensitive information. Arizona's system sets forth the intention that patients actually understand the existence and the reason for the HIO and can build its enrollment by automatically entering patient information. Arizona has also taken note of patients' desire to limit some categories of information from the HIE, yet this system may undermine clinical care if providers are not aware that a patient's record from the HIE is incomplete and missing crucial pieces of information that would influence their decision-making. Lastly, Arizona's provision

---

[82] *What is Arizona Health-e Connection?*, ARIZONA HEALTH-E CONNECTION, http://www. azhec.org/ (last visited May 23, 2012).

[83] ARIZ. REV. STAT. § 36-3801 (2012).

[84] ARIZ. REV. STAT. § 36-3804 (2012).

[85] ARIZ. REV. STAT. §§ 36-3802, 36-3803 (2012).

[86] ARIZ. REV. STAT. § 36-3803.

[87] ARIZ. REV. STAT. § 36-3807 (2012).

[88] ARIZ. REV. STAT. § 36-3805 (2012).

for the disclosure of health information provides two potentially conflicting standards and may pose a confusing barrier to secondary uses of data in the HIE.

V. HOW GRANULARITY CAN IMPACT PUBLIC HEALTH, RESEARCH USE, AND PATIENT TRUST

As HIOs examine policy choices relating to consent models and options for granularity, they must also consider how these permutations and will intersect with long terms goals of the HIO. If the HIO or state law adopts the HITECH Act's objective to use patient information for research, policymakers must be cognizant of the delicate interplay between using robust patient data (including sensitive information) for research purposes while preserving patient trust, maintaining their privacy, and minimizing potential breaches of that sensitive information.

Information amassed in the HIE could be used for a variety of secondary purposes including quality improvement, public health, and research.[89] Public health researchers could use patient information in the HIE for health assessment, promotion of population health, and policy development.[90] Public health agencies could use the information in HIEs for tracking and minimizing the spread of disease, as well as aiding in disaster planning efforts.[91] Health services researchers could track patient information in the HIE to examine incidence and prevalence of disease and treatment outcomes to gather data to assist in more effective treatment of disease.[92] However, if HIOs by default policy fully exclude all sensitive information and do not enter it into the HIE, then researchers will be hindered from using a valuable potential set of data that could otherwise be accessible to researchers by a consent mechanism. If HIOs provide patients the option to fully exclude categories of patient information from the HIE, then patients' varied choices to include or exclude their

---

89 Francis, *supra* note 2, at 44.

90 Bomash, *supra* note 23, at 120.

91 *Id.* at 121-22.

92 *Id.*

sensitive information will carry over to unrepresentative data sets for these categories of sensitive diseases and conditions.[93] If HIOs provide patients options for granular control by including masked and flagged sensitive information in the HIE, the HIO could develop policies and procedures relating to patient consent and researcher access to that information, providing more representative data sets and potential public health and research benefits. Indeed, Professor Goodman argues that physicians have a duty to use patient information for public health purposes and contribute to knowledge that will instruct future clinical care. [94]

Importantly, patients must trust that the HIO will not misuse the patient information it holds or clinical care, potential public health advances, and research benefits will suffer.[95] Health law attorney Kari Bomash has discussed extensively the synergy between patient privacy and the ability to derive public health information.[96] If patients do not believe the HIO has provided appropriate choices and safeguards for their private and sensitive medical information for secondary uses, they lose trust in the provider and HIO.[97] Some proposals argue that we must override patients' desire to withhold their health information for research because the public simply cannot appreciate the benefits their medical information holds for research and mere use of health records does not pose palpable harm to the individual patient.[98] Such thinking is not only remarkably paternalistic and offensive, but ignores the delicate balance of trust sustaining the evolving

---

[93] *See* Barbara Evans, *Much Ado About Data Ownership*, 25 HARV. J.L. & TECH. 69, 76 (2011) (discussing the use of large datasets in large scale informational research and the impact of individual refusal).

[94] Goodman, *supra* note 23 (arguing that physicians have a duty to use patient information for public health research and return these results to patients in the form of better clinical care).

[95] Bomash, *supra* note 23, at 121-22.

[96] *Id.* at 120-23.

[97] *Id.* at 121-22; Rothstein, *Improve Privacy*, *supra* note 72, at 510-11.

[98] Franklin G. Miller, *Research on Medical Records Without Informed Consent*, 36 J.L. MED. & ETHICS 560, 561-65 (2008).

physician-patient relationship in an age of growing health information technology as well as growing risks of wrongful disclosures (discussed infra Section VI). As Professor Rothstein has aptly noted, if patients feel betrayed by their providers and believe their privacy is compromised, they may become anxious, withhold critical information from their provider, and become reluctant to seek care.[99] Professor Rothstein correctly emphasizes that it is good public policy to promote public health, but it is also imperative that we work to prevent nonmedical harm to patients such as embarrassment and stigma.[100] Importantly, the populations with the most precarious trust such as those with stigmatizing health conditions and minority populations facing high rates of chronic disease may be most in need of the efficient and effective clinical care and research updates that HIOs can eventually provide.

VI. HIEs: A NEW MARKET FOR WRONGFUL DISCLOSURES AND SECURITY BREACHES OF PATIENT INFORMATION

As HIOs amass medical information, including potentially stigmatizing categories of sensitive information, privacy advocates and policymakers have discussed the growing potential for wrongful disclosures and security breaches of this information.[101] By nature and design, EHRs contain comprehensive information relating to patient history, patient demographic information, and patient identifying information including as social security number and billing information. Unlike paper records that may contain pieces of information on select patients in a physical location, EHRs are digitally stored in the aggregate, which eases the ability of an individual to download and replicate the information.[102] The sheer amount of information contained in the HIE including

---

[99] Rothstein, *Improve Privacy*, *supra* note 72, at 510.

[100] Rothstein, *E-Health Hazards*, *supra* note 1, at 11.

[101] Peel, *Your Medical Records Aren't Secure*, *supra* note 38; Bomash, *supra* note 23, at 122.

[102] Keith A. Bauer, *Privacy and Confidentiality in the Age of E-Medicine*, 12 J. HEALTH CARE L. & POL'Y 47, 52 (2009).

names, social security numbers, billing information, and comprehensive medical information creates a new market for a variety of wrongdoing by businesses and opportunistic individuals. This increase in the amount of information available in one electronic location requires an evolving analysis of privacy and security risks, and the recognition that thieves may begin to calculate and target the large collection of medical information held by HIOs.[103] Specifically, HIOs that automatically include all patients in the RLS and patient information in the HIE should explain risks of potential breach to patients.[104] HIOs that include categories of sensitive information in the HIE, even if hidden and masked in the system, should also take care to communicate the potential for wrongful disclosure of this sensitive information.

Examples of wrongful disclosures range from isolated incidents involving one or a few medical records, to unintentional system security breaches, to large-scale calculated breaches. Healthcare employees may wrongfully disclose medical information for personal gain or curiosity.[105] Numerous headlines have described how employees mistakenly published patient records on the Internet or lost a USB key, allowing unauthorized individuals access to highly personal information.[106] The amount of patient information in HIEs also opens a market for discriminatory use of medical information by employers and insurers seeking to employ only healthy employees or attempting to reduce costs.[107] Patients with sensitive medical conditions or chronic health conditions may be especially wary of HIOs holding their information if they

---

[103] Consolidated Amended Class Action Complaint at 6, 21-22, Gaffney v. TRICARE Management Activity, No. 1:11-cv-01800-RLW (D.C. Cir. Feb. 21, 2012), *available at* http://cdn.govexec.com/media/gbc/docs/pdfs_edit/031412bb1a.pdf [hereinafter TRICARE Complaint].

[104] *See* Stanley C. Ball, *Ohio's "Aggressive" Attack on Medical Identity Theft*, 24 J.L. & HEALTH 111, 123-29 (2011) (discussing security breach and notification rules); Hoffman, *supra* note 1, at 1555-61.

[105] Ayres, *supra* note 18, at 970-72.

[106] *See generally* Ayres, *supra* note 18; Ball, *supra* note 104, at 114.

[107] Bomash, *supra* note 23, at 122; Ayres, *supra* note 18, at 973.

believe employers and insurers could gain (even unauthorized) access to these records. Finally, individuals can steal information by obtaining the physical source, such as a computers or hard drive, or illegally hack into information stored in an electronic system.[108]

One recent breach exemplifies the growing risk of security breaches and the sheer number of potentially affected individuals. In September 2011, TRICARE, which provides health benefits to the military and their families, reported a massive security breach affecting almost five million beneficiaries.[109] According to media reports, the breach occurred through the theft of backup computer disks holding addresses, health information, and social security numbers.[110] This incident is particularly notable not only because of the astounding amount of victims affected by the breach, but also the factual circumstances surrounding the theft. Plaintiffs allege that the incident constituted a carefully calculated, targeted, and executed attempt to steal the specific information contained in the backup disks, which plaintiffs estimated to be worth billions of dollars.[111]

Media reports show both large-scale data breaches and isolated incidents have resulted in identity theft, and the newer form of identity theft, medical identity theft.[112] Bad actors may hack into storage systems to gain access to patients' personal and medical information to sell at a hefty price on the black market, leaving these victims to investigate and mitigate damage to their finances, credit, and even medical records and insurance.[113] Apart from general identity theft, individual medical identity theft

---

[108] Ball, *supra* note 104, at 114.

[109] *Privacy and Security: Individuals Affected by TRICARE Data Breach Allege Possible Fraud*, IHEALTHBEAT.COM (March 15, 2012), http://www.ihealthbeat.org/articles/2012/3/15/individuals-affected-by-tricare-data-breach-allege-possible-fraud.aspx (last visited Nov. 5, 2012).

[110] *Id.*

[111] TRICARE Complaint, *supra* note 103, at 21-22.

[112] Katherine Sullivan, *But Doctor, I Still Have Both Feet! Remedial Problems Faced by Victims of Medical Identity Theft*, 35 AM. J.L. & MED. 647 (2009); Ball, *supra* note 104, at 117-20.

[113] Sullivan, *supra* note 112, at 650-52.

occurs when an individual assumes another person's identity to receive medical services and bills the victim's insurance.[114] Individuals may also steal information from multiple parties to commit medical identity theft and defraud third party payers by billing the victim's insurance for services and procedures that the victim did not actually receive.[115] In addition to sorting out fraudulent billing claims, victims may face negative implications for their credit as a result of billing errors. Furthermore, insurers processing the fraudulent claims may bill the victim for deductibles, co-payments and other costs. [116] The victim's insurance company may also deny or delay coverage of benefits to the victim, or even refuse further benefits if the company decides the patient has exhausted the policy's coverage. [117]

Problematically, providers likely add the fraudulent information into the victim's medical record, which impairs subsequent providers' ability to properly treat the real patient and can result in dangerous medical errors.[118] As HIOs continue to build their presence, the possibility that the provider enters the identity thief's fraudulent information into the permanent comprehensive patient record becomes even more likely, and raises the possibility that the fraud will directly impact the victim's subsequent medical care. Integration of fraudulent information into the victim's patient chart is especially dangerous if care occurs during an emergency situation where the victim cannot notice and correct the errors.[119]

---

114 *Id.* at 650-51.

115 *Id.*

116 Ball, *supra* note 104, at 117-20.

117 *Id.*

118 Sullivan, *supra* note 112, at 650-52.

119 *Id.*

VII. IMPLICATIONS OF BUILDING HIOS WITH OPTIONS FOR GRANULARITY, EFFECTS ON CLINICAL CARE, AND POTENTIAL PROVIDER LIABILITY

Adoption of EHRs and interoperable HIEs aims to allow providers to more effectively and efficiently care for their patients. By definition, a provider should be able to access a patient's EHR to locate longitudinal and comprehensive information about the patient. However, adopting a system of granularity that fully excludes patient information from the HIE (either never entered into the HIE or its existence fully hidden from subsequent providers) does not satisfy these specific clinical care aims of an HIE. Furthermore, a physician who accesses a patient's records from the HIE may mistakenly believe the record is complete, leading the physician to make inappropriate treatment decisions or prescribe contraindicated medications. Providers must be aware of variable clinical duties and potential liability connected to these choices for granular control.

This scenario could potentially expand physician liability for medical malpractice in negligence actions for physicians at two points of care interacting with the patient, particularly where physicians hold discretion in deciding whether or not to add sensitive records to the HIE or access sensitive records from the HIE. Professors Hoffman and Podgurski have extensively discussed liability implications for physicians arising from the adoption of EHRs, noting that shifting standards of care and the sheer amount of information physicians must process for effective care poses significant challenges for physicians attempting to navigate clinical care decisions.[120] In a traditional negligence action, patients who believe the physician was negligent must establish: (1) a duty of care owed by the defendant to the plaintiff; (2) breach of that duty through conduct that fails

---

[120] *See* Hoffman, *supra* note 1 (discussing physician and institutional liability associated with the adoption of EHRs); *see also* Sandeep Mangalmurti et al., *Medical Malpractice Liability in the Age of Electronic Health Records*, 363 NEW ENG. J. MED. 2060 (2010) (discussing the evolution of medical malpractice liability relating to the adoption of EHRs).

to meet the applicable standard of care; (3) harm or injury; and (4) a causal link between the breach of duty and the plaintiff's injury.[121] Imagine the following scenario: Patient could show that Physician A who treated Patient for Sensitive Condition owes Patient the duty to consider the impact of not entering a part or the whole Sensitive Treatment Record into the HIE as part of Patient's ongoing care and management of Sensitive Condition. If more physicians begin to enter sensitive records into HIEs, this practice could become the new standard of care, and Physician A's decision to withhold Sensitive Record from HIE may constitute a breach of that duty owed to Patient. [122] If Patient can show that but for Physician A's decision to exclude Sensitive Record that Patient would not have sustained an injury (such as medication interaction or contraindicated care) in a subsequent clinical care encounter with Physician B and Patient actually sustained such an injury, Patient could bring a medical malpractice liability lawsuit against Physician A for negligence. Patient could similarly apply this rationale to subsequent treatments by Physician B. If Physician B does not request Patient's Sensitive Records separately, through the HIE if the Sensitive Records are masked, or fails to integrate the information from Sensitive Records and the failure to consider Patient's Sensitive Records proximately causes Patient harm, Patient may also bring a negligence action against Physician B.

In addition to one-on-one interactions between physicians and patients, adopting a system of granularity that fully excludes patient information from the HIE or enters sensitive information based on provider or patient discretion carries implications for anticipated features of EHRs relating to clinical decision support. In theory, medication dosages, best practice guidelines, and treatment

---

[121] W. PAGE KEETON ET AL., PROSSER & KEETON ON THE LAW OF TORTS (5th ed. 1984).

[122] *See* Thomas McLean, *EMR Metadata Uses and E-Discovery*, 18 ANNALS HEALTH L. 75 (2009) (discussing use of EMR metadata for medical malpractice liability to establish physician knowledge and practice, and to use metadata to show general custom in the profession).

suggestions are based on gathering clinical data from a broad representative spectrum of patients to understand the effectiveness of particular treatments and courses of action.[123] Systems for granularity could skew collection of patient data in two ways. First, an HIO could use a self-selecting sample of data based on some patients who choose to include their sensitive information in the HIE, resulting in an unrepresentative sample population, which would correspondingly distort data outcomes. Second, an HIO may choose to exclude all patient data relating to sensitive conditions from clinical decision support features, which would result in clinical decision support data that cannot account for the interplay between patients' sensitive conditions and other medical needs. Such a system may recommend inappropriate medications that would be contraindicated for some patients based on other co-existing conditions such as depression or alcohol addiction, or suggest an incorrect diagnosis based on a patient's symptoms that could otherwise be attributed to the patient's sensitive co-existing condition. To minimize liability, providers who utilize clinical decision support guidelines should proceed cautiously and assess whether guidelines for a particular diagnosis or medication dosage are appropriate for each particular patient and whether the patient history shows any sensitive conditions that would alter the physician's clinical assessments.

Finally, different options for granularity influence how identity theft may manifest, its corresponding implications on clinical care, and provider liability. First, if an HIO excludes sensitive information from its HIE then medical identity thieves may strategically target patients in this HIE to obtain specific "sensitive" costly goods and services because they know that a record of their receipt of these services will not show up in the patient's file and the patient will not be alerted to the theft until months later when the patient is billed by insurance. As with other forms of medical identity theft, providers must bolster their data security to lessen the potential for general identity theft and

[123] Hoffman, *supra* note 1, at 1538-42; Mangalmurti et al., *supra* note 120, at 2062, 2064.

increase point of contact identity matching during patient care interactions to minimize institutional liability. Second, if an HIO includes sensitive information providers must be aware of the possibility that information in the patient's chart relating to a sensitive condition may not reflect the patient's actual medical history. Providers should take care to scan areas of patients' comprehensive EMR and mention potential areas that influence their clinical decision-making to ensure patient's verbally recounted history accurately matches patient records as a precaution to minimize physician liability.

VIII. POLICY CONSIDERATIONS AND CONCLUSION

The complexities and disparities among state law treatment of sensitive information poses the challenging question of how to balance protecting patients' deeply private sensitive medical records while building HIEs that can increase the effectiveness of patient care. As policymakers and emerging HIOs consider options for granularity, they should consider whether the policy choice interferes with the overarching purpose of the HIE. That is, a patient's EHR is designed as a comprehensive medical history reference so physicians can make a fully informed diagnosis, offer appropriate options for treatment, and check for contraindications or potential negative interactions. If an HIO fully excludes sensitive information from its HIE, physicians could miss crucial information relating to the patient's state of mind, whether the patient's decision-making capacity is influenced by external factors, or whether information in the patient's sensitive record would alter the physician's clinical judgment for diagnosis and appropriate treatment actions.

Privacy advocates warn of the embarrassment and stigma arising from disclosure of sensitive medical information and the risks of wrongful disclosures. These concerns should not be dismissed, but instead we should design a system that can tailor access to the information and release it when necessary. Importantly, patients should understand both the risks and benefits of

participating in the HIE and why sequestering sensitive records from the HIE can negatively effect their clinical care. As a policy objective, the HIO should strive to educate patients on the benefits and risks of placing their information in the HIE and design a system where physicians can access their comprehensive records with their knowledge and permission. Operational models demonstrate that patients want to understand and choose whether to participate in the HIE and assume the benefits and risks, which could be accomplished by consent or opt-out. An HIO could limit access to the sensitive information with an added layer of security but still hold the sensitive information as a reference. If an HIE contains sensitive information in masked and flagged form, physicians can initiate a conversation with patients about the information, request access when appropriate, and gain access in an emergency. This system would limit disclosures of sensitive information to respect patients' privacy while striving to facilitate trust and communication. Patient privacy should not come at the expense of a physician's ability to accurately assess patient history and effectively treat the patient, which could cause the patient tangible and substantial physical harm.

Policymakers and HIOs should consider how choices for granularity affect the long-term goals of the HIE, its ability to sustain patient trust, and serve as an effective resource for physicians to provide effective clinical care. Despite the potential promises for advancing clinical care and using the HIE data for research; HIOs must recognize that the ability to derive public health information is intricately tied to patient trust. Using patients' health information without their knowledge or consent will undoubtedly result in patients' loss of the trust in the HIO and their providers and accordingly, HIOs should not adopt policies that ignore or override patients' desires not to share their health information in the HIE or for research. Given this large amount of patient information in the HIE, HIOs must also anticipate evolving risks of wrongful disclosure and potential for security breaches. HIOs should carefully communicate these risks to patients, and take steps to

mitigate wrongful disclosures and intentional breaches. Finally, providers should consider how varying options for granularity could impact their ability to effectively treat patients by integrating medical history and clinical decision support features and consider future projections of potential provider liability.