BOMASH K. PRIVACY AND PUBLIC HEALTH IN THE INFORMATION AGE: ELECTRONIC HEALTH RECORDS AND THE MINNESOTA HEALTH RECORDS ACT. MINN. J.L. & TECH. 2009 10(1):117-41.

Privacy and Public Health in the Information Age: Electronic Health Records and the Minnesota Health Records Act

Kari Bomash*

I. INTRODUCTION

In 2004 President George W. Bush announced a new federal initiative to develop electronic health records ("EHR") for every American by 2014 because of their tremendous promise to reduce medical errors, reduce administrative costs in the health care system, and improve public health research.[1] In response to President Bush's announcement, Minnesota Governor Tim Pawlenty, in 2005, supported a statewide mandate that every health care provider in Minnesota would have EHRs by 2015.[2] One of the first pieces of legislation Minnesota passed to meet the 2015 mandate was the Minnesota Health Records Act ("MHRA"), which was hailed as creating an "electronic superhighway for medical records."[3]

* Kari Bomash, J.D., M.P.H., is an Associate in the Health Law Group at Dorsey & Whitney. I would like to thank Susan Foote for her understanding, patience, and guidance, and Donna McAlpine for helping me to finish this project despite enormous challenges.

1. *See, e.g.*, Laura Dunlop, *Electronic Health Records: Interoperability Challenges Patients' Right to Privacy*, 3 SHIDLER J. L. COM. & TECH. 16, 16 (2007).

2. MINN. STAT. ANN. § 62J.495 (West. Supp. 2008); MINN. DEPT. OF HEALTH, FINAL REPORT ON PRIVACY AND SECURITY BARRIERS TO, AND SOLUTIONS FOR, THE ELECTRONIC EXCHANGE OF HEALTH INFORMATION (2007), *available at* http://www.health.state.mn.us/e-health/mpsp/solutionsrpt.pdf [hereinafter *Solutions Report*]; Summary of 2007 HHS Omnibus Bill, http://www.health.state.mn.us/divs/opa/07legsumm.html (last visited Nov. 17, 2008).

3. Lorna Benson, *Network Will Link Patient Records,* MINN. PUB. RADIO, Sept. 10, 2007, *available at* http://minnesota.publicradio.org/display/web/2007/09/10/healthrecords; *see also* MINN. DEPT. OF HEALTH, FROM VISION TO ACTION: THE MINNESOTA E-

The MHRA re-codified existing state law regarding the disclosure of medical records and added three new features which were developed in an attempt to remove patient consent-related barriers from the development and implementation of EHRs.[4] Those features are: (1) Record Locator Services ("RLS")—electronic indexes stating the physical location of a patient's records; (2) "representation of consent," which allows a disclosing provider to accept a requesting provider's statement that there is valid consent for record disclosure in lieu of a signed consent form from the patient; and (3) liability for illegal disclosure for a "bad actor."[5] Privacy advocates, echoing the concerns of some media and scholars, argued before the Minnesota State Legislature that the MHRA weakens patient privacy protections for medical records by encouraging EHR development.[6]

This article analyzes whether the MHRA adequately protects patient privacy while moving Minnesota toward its 2015 goal. First, the article explores the importance of patient privacy protection as a public health policy in the context of EHRs. Second, it briefly outlines the legal landscape of EHR privacy regulation. Third, the article considers whether the previous Minnesota medical records disclosure law was a barrier to EHR implementation. Fourth, it examines whether public health needs were adequately considered in the MHRA and whether the law balances individual privacy with EHR development. Finally, the article considers whether and how the MHRA should be amended to better meet public health privacy goals.

II. BACKGROUND

A. ELECTRONIC HEALTH RECORDS AND PATIENT CONSENT OF

HEALTH INITIATIVE (2008), *available at* http://www.health.state.mn.us/e-health/legrpt2008.pdf [hereinafter *E-Health Initiative*].

4. *Minnesota Health Records Act of 2007: Hearing on H.F. 1726 Before H. Comm. on Public Safety and Civil Justice*, 85th Leg. Sess. (Minn. 2007) (statement of Jim Golden), *available at* http://www.house.leg.state.mn.us/audio/archivescomm.asp?comm=6000&ls_year=85) [hereinafter *Mar. 21, 2007 hearing*].

5. *Id.*

6. *See, e.g.*, *Minnesota Health Records Act of 2007: Hearing on S.F. 1701 Before S. Comm. on the Judiciary*, 85th Leg. Sess. (Minn. 2007), *available at* http://www.senate.leg.state.mn.us/schedule/schedule.php?date=5/1/2007&type=weekly&ls=85 [hereinafter *May 1, 2007 hearing*].

RECORD DISCLOSURE

Electronic medical records (EMRs) generally refer to any medical record or part of a medical record that is kept in an electronic format.[7] Thus, an EMR could include any or all of the following: lab results, x-rays, prescriptions, physicians' notes, or research on a specific patient.[8] An EHR is an interoperable EMR. Currently, most EMRs are not interoperable, even if networks have purchased EMR technology from the same vendor.[9] Interoperable EMR technology has not thus far developed because: (1) there are no agreed-upon data standards for interoperability; (2) there is not a consistent incentive scheme to encourage interoperable development; and (3) there are increasing technological differences between EMR databases as vendors build more specialized systems for different health care networks.[10]

At present, patient privacy protection of medical records is controlled mostly by patient consent laws that define how and when a patient must consent before a physician may disclose the patient's medical records to anyone else.[11] Consent is a concept that works relatively well to protect paper records because of the physical size of medical records, and the fact that most are stored piecemeal at multiple medical facilities.[12] The difficulty of mining paper records for information limits the

---

7. Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, U. ILL. L. REV. 681, 700–07 (2007)("There are great advantages to using electronic medical records more extensively, both within the offices of individual providers, where they are known as electronic medical records (EMRs), and also when such records are linked across multiple providers, in which case they are known as electronic health records (EHRs)."); s*ee generally* Elisabeth Belmont & Adele A. Waller, *The Role of Information Technology in Reducing Medical Errors*, 36 J. HEALTH L. 615, 616 (2003); Brent James, *E-Health: Steps On The Road to Interoperability*, HEALTH AFFS. , Jan. 19, 2005, http://content.healthaffairs.org/cgi/content/full/hlthaff.w5.26/DC1.

8. *See generally* Belmont & Waller, *supra* note 7.

9. *Id.* at 617–618.

10. Peter Pharow & Bernd Blobel, *Specific Interoperability Problems of Security Infrastructure Services*, *in* 3 MED. & CARE COMPUNETICS 349, 360–61 (L. Bos et. al eds. 2006); Robert Malone, Note, *Health Information Technology: Transforming the Healthcare Industry for the 21st Century*, 3 OKLA. J. L. & TECH. 36, 3 (2007).

11. Alicia Ouellette & Jacob Reider, *Practical, State, and Federal Limits on the Scope of Compelled Disclosure of Health Records*, 7 AM. J. OF BIOETHICS 46, 46–47 (2007).

12. *Id.*

utility and consequences of theft.[13] In an interoperable system where these organizational issues no longer exist, patient consent may be only one piece of a broader scheme of privacy regulation designed to more adequately protect the patient from foreseen and unforeseen uses of patient data.[14]

B. PATIENT PRIVACY PROTECTION AS A PUBLIC HEALTH AIM

The creation of an EHR network that allows researchers to access de-identified population-level data would aid public health in all three of its core functions: assessment, assurance, and policy promotion. Privacy protection is integral to ensuring that high-quality data are collected by such a network. Therefore, patient privacy is a legitimate public health aim. Moreover, security breaches of EHRs could have broad social consequences which justify government regulation to protect patient privacy.

An interoperable system that allows public health researchers to access de-identified population level data would allow for better and faster assessment of diseases that strike the general population and sub-populations.[15] It would also allow for non-industry assessment of competing treatments and faster development of evidence-based physician treatment guidelines.[16]

An EHR network can help assure good population health by allowing the Centers for Disease Control or local health departments to track disease outbreaks in near real time.[17] This development may reduce the time it takes to stop the spread of the disease, and thus improve assurance that the disease can be contained.[18] An EHR network also has public health benefits for emergency and disaster planning.[19] It would allow relocated patients to access complete medical records, regardless of the physical state of their physician's

13. *Cf.* Terry & Francis, *supra* note 7, at 700–07.

14. *Id.*

15. Roger S. Magnusson, *The Changing Legal and Conceptual Shape of Health Care Privacy*, 32 J.L. MED. & ETHICS 680, 685–87 (2004).

16. *Id.*

17. *Id.* at 686.

18. *See id.*

19. Robert Malone, Note, *Health Information Technology, E-Prescribing and Hurricane Katrina: Could Electronic Health Records Have Made A Difference?*, 3 OKLA. J. L. & TECH. 38, 9 (2007).

office, and thus minimize any interruption of care that might result from a disaster.[20] Therefore, EHRs would lessen the negative health impacts due to relocation. Finally, an EHR system can help improve the daily care that a patient receives because it can be designed to prospectively check prescription drug interactions and to facilitate the execution of treatment guidelines so that patients will receive the most appropriate, evidence-based care.[21]

An EHR network would aid in policy promotion because it could provide more accurate data regarding the incidence and prevalence of disease, the effectiveness of alternative treatments for those diseases, and the treatment costs.[22] Such information will help health agencies prioritize health agendas, advocate for funding and research, and plan cost-effective interventions that improve the public's health.

Promoting and protecting the privacy of patient medical records is vital to maintaining a functioning public health system.[23] Two renowned scholars in public health and law, Lawrence Gostin and James G. Hodge, have developed the theory that there is a synergistic relationship between privacy protection and public health benefits deriving from shared information.[24] They argue that successful information technology for public health depends upon strong privacy protection because public health entities (usually governmental) cannot function without the support and trust of individuals.[25] To maintain that trust, individuals must believe that public health agencies will not misuse or abuse health

---

20. *Id.* at 6–7.

21. *See* June M. Sullivan, *Recent Developments and Future Trends in Electronic Medical and Personal Health Records*, 19 HEALTH L. 16, 16 (2007); Terry & Francis, *supra* note 7, at 692–93.

22. MINN. DEPT. OF HEALTH, PROTECTING COMMUNITIES THROUGH IMPROVED PUBLIC HEALTH INFORMATION SYSTEMS (2007), *available at* http://www.health.state.mn.us/e-health/mnphin/legrpt2007.pdf [hereinafter *Information Systems Report*].

23. Lawrence O. Gostin & James G. Hodge, Jr., *Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule*, 86 MINN. L. REV. 1439, 1440 (2002); James G. Hodge, Jr., *Health Information Privacy and Public Health*, 31 J. L. MED. & ETHICS 663, 663 (2003) [hereinafter Hodge I]; James G. Hodge, Jr., *National Health Information Privacy and New Federalism*, 14 NOTRE DAME J.L. ETHICS & PUB. POL'Y 791, 791 (2000) [hereinafter Hodge II].

24. Gostin & Hodge, *supra* note 23, at 1441–43.

25. *Id.* at 1442.

information and will strongly protect patient data.[26] Otherwise patients may not wish to participate fully or they might withhold sensitive information which may affect the individual patient's treatment and, at a population level, skew research results and policy proposals that result from that research.[27] In other words, in order to get accurate data that can lead to valid research and policy development, public health agencies must be able to protect the individual privacy of those records.

The privacy of EHRs also has public health ramifications due to the potential scale of security breaches. Currently, paper records are not very secure.[28] Someone intent on stealing records could easily walk into most clinics and walk out with files.[29] However, such a theft is limited to affecting the individuals whose records are stolen because of the physical size of the files and the fact that they are housed in disparate locations. Further, there is not a great market for this medical information because of the difficulty in amassing a large volume of records. Electronic records may actually be more secure than paper records, if for no other reason than that clinics would have password-protected systems to access them.[30] It would take a higher level of skill to hack into even a moderately secure system than to walk into an office and steal paper records. The difference is that should someone steal electronic records, they could potentially steal a huge number of them and they could steal an entire record rather than just a piece.[31] The scope of the theft creates the possibility of producing markets for medical information to employers or insurance companies who want to reduce costs, or to medical companies that will mine that data for marketing health products, or to health care entities themselves who want to win patients.[32] These consequences have much broader social implications than the theft of individual files because the data could then be used for private financial gain rather than for legitimate public health purposes.

A full-fledged public health privacy policy should be

26. *Id.*
27. *Id.* at 1551–52.
28. *See May 1, 2007 hearing*, *supra* note 6; Sullivan, *supra* note 21, at 17.
29. Sullivan, *supra* note 21, at 17.
30. *Id.*
31. Magnusson, *supra* note 15, at 685.
32. *Id.*

developed because privacy protection is integral to continuing and developing EHR networks. The absence of a well-designed policy means that there are no consequences for data misuse because such misuse is not prohibited. The absence of a privacy policy will not prevent EHR development. It will simply mean that whether and what kind of privacy protections are used with EHR technology will be determined by industry instead of by government and public health agencies.

A review of the literature ultimately shows three key areas on which a public health privacy policy should focus: patient consent, data security standards, and data use. The first issue is that of patient consent to record disclosure and how that process will and will not work with EHRs.[33] The second issue is the assumption that data will not be secure.[34] This assumption suggests that any privacy policy for EHRs must include data security requirements to protect data beyond a patient's consent. The third issue considers how medical information will be used.[35] This concern suggests that public policy must define acceptable and unacceptable data uses; it must also determine consequences for data abuse in an attempt to minimize the creation of markets for inappropriate data use. The issues of consent, data standards, and information use should be developed simultaneously in relation to each other as the protections of each may change depending on the protections of the others. For example, the consent process may change depending on the data security requirements. Likewise, the data security requirements might change based on the intended data use.

In order to protect the privacy of records and to meet public health aims, government can either: (1) build a public infrastructure for the exchange of records and extrapolation of

---

33. *See, e.g.*, Mark A. Rothstein & Meghan K. Talbott, *Compelled Disclosure of Health Information: Protecting Against the Greatest Potential Threat to Privacy*, 295 JAMA 2882 (2006); Terry & Francis, *supra* note 7; Kristin E. Schleiter, *The Dinosaur in the Office: A Consideration of the Technical and Ethical Issues Surrounding the Adoption of Digital Medical Data and the Extinction of the Paper Record*, 16 ANNALS HEALTH L. 353, 356–57 (2007).

34. *See, e.g.*, Latour Lafferty, *Medical Identity Theft: The Future Threat of Health Care Fraud Is Now*, 9 J. HEALTH CARE COMPLIANCE 11, 11 (2007); Magnusson, *supra* note 15; Rothstein & Talbott, *supra* note 33.

35. *See, e.g.*, Rothstein & Talbott, *supra* note 33; Terry & Francis, *supra* note 7.

data that will protect individual privacy or (2) develop a regulatory framework of privacy and security requirements by which private industry may act. These solutions differ from policy that promotes EHRs for individual medical benefit because those policies focus more on organizational-level privacy regulation (mostly via patient consent) and technology adoption. A public health privacy policy includes patient consent, but also regulates the technology industry directly to provide technological security. The MHRA is an indication that Minnesota has decided to develop regulation for private entities rather than to build the EHR infrastructure itself.

C. LAYERS OF INTERLOCKING REGULATION

Currently there is no cohesive medical data privacy policy in the United States.[36] Instead, laws are divided between state and federal governments and organized by different categories of regulation (such as consent and data standards).[37] Most of the discussion of privacy protection laws and health records focuses on whether the Health Insurance Portability and Accountability Act ("HIPAA") provides sufficient protection of patients' medical records, or alternatively, how HIPAA has been or could be changed to encourage EHR networks.[38] As a federal law, HIPAA can provide uniform rules across states for EHR privacy. However, HIPAA is considered a regulatory "floor," meaning that all states must at a minimum provide HIPAA protections of medical records, although states are free to provide more stringent protections.[39] Therefore, state regulation such as Minnesota's may have a greater impact upon the development of EHR technology and privacy within the state. In fact, many state laws require greater levels of protection for medical records than does HIPAA.[40] As a result, the nationwide privacy protection of medical records is a patchwork of different laws and standards which in and of

36. *See* Terry & Francis, *supra* note 7, at 683.

37. *See* Nancy J. Brent, *The Use and Misuse of Electronic Patient Data*, 28 J. OF INFUSION NURSING 251, 252–54 (2005).

38. *See, e.g.*, *id.*; Bridget M. Carney, *Breaches of Confidentiality and the Electronic Community Health Record: Challenges for Healthcare Organizations and the Community*, 13 H.E.C. FORUM 138, 138 (2001); Gostin & Hodge, *supra* note 23; Malone, *supra* note 10.

39. Brent, *supra* note 37; Carney, *supra* note 38; Gostin & Hodge, *supra* note 23; Malone, *supra* note 10, at 4.

40. Terry & Francis, *supra*, note 7, at 707.

itself challenges the creation of and participation in a national EHR network.

1. Minnesota's Data Security Standards

Health data standards have been considered as part of Minnesota's overall privacy protection scheme.[41] Recently the Minnesota Department of Health ("MDH"), the agency that coordinates EHR development and regulation, stated that it has enacted interoperability data standards.[42] There are data standards for a few special areas such as e-prescribing.[43] However, broad security standards applicable to all portions of an EHR have yet to be developed. One committee has recommended that Minnesota adopt federal recommendations when such recommendations are made.[44] The federal government may ultimately make an interoperability data standards recommendation through various private EHR technology licensing entities such as the Certification Commission for Health Information Technology ("CCHIT") and the Health Information Technology Standards Panel ("HITSP"). However, the federal office in charge of EHR development, the Office of the National Coordinator for Health Information Technology, essentially coordinates regional efforts to develop EHR technology.[45] Consequently, the cautious recommendation to wait for federal guidance does not significantly move the state towards developing data security standards for EHRs.

2. Consent: The Minnesota Health Records Act

The MHRA re-codified and modified pre-existing Minnesota patient consent laws for the disclosure of medical records in three key areas: (1) defining and regulating an RLS; (2) developing the concept of a representation of consent; and (3) shifting liability to a "bad actor" in the case of an unlawful

41. *See, e.g.*, *E-Health Initiative*, *supra* note 3.

42. *Id.* at 6–7.

43. *See* MINN. STAT. § 152.126 (Supp. 2007).

44. *See E-Health Initiative*, *supra* note 4. The E-Health Committee is comprised of various EHR stakeholders that recommends policies and laws to the legislature to aid in EHR development and implementation.

45. U.S. Dept. of Health and Hum. Servs., Office of the National Coordinator for Health Information Technology: Mission, http://www.hhs.gov/healthit/onc/mission (last visited Nov. 17, 2008).

disclosure.[46] The legislative history shows that the Minnesota State Legislature intended that the MHRA would encourage EHR development while protecting patient privacy.[47] It also shows that the legislature failed to consider broader EHR and privacy policies when developing the MHRA.[48] In fact, of the factors identified above (patient consent, data security standards, and data use), the MHRA and preceding debates focused only on the specific patient consent process.[49]

i. The Record Locator Service

The MHRA authorizes the development of RLSs, which in essence are indices of the physical locations of the patients' records.[50] An RLS is owned by a Health Information Exchange ("HIE") which is a legal arrangement between various health care entities (including payors) that have agreed to share information.[51] Any member of the HIE with information about patients can enter non-clinical identifying information about the patient into the RLS without the patient's consent.[52] Thus, a payor, the MDH, or provider with records about a patient can enter enough information to uniquely identify the patient (name, date of birth, parents' names, etc.) and can indicate that they have records for that patient. The RLS does not contain the actual patient records; it only indicates where the patient's records can be found.[53]

Only providers may access the RLS to get a record's

46. *See* MINN. STAT. §§ 144.291, 144.293, subdiv. 2, 144.298 (Supp. 2007).

47. *See, e.g.*, *Minnesota Health Records Act of 2007: Hearing on H.F. 1726 Before the H. Comm. On Health and Human Services*, 85th Leg. Sess. (Minn. 2007), http://www.house.leg.state.mn.us/audio/ls85/healthpol031307.asx [hereinafter *Mar. 13, 2007 hearing*]; *Minnesota Health Records Act of 2007: Hearing on H.F. 1726 Before the H. Comm. On Health and Human Services*, 85th Leg. Sess. (Minn. 2007), http://www.house.leg.state.mn.us/audio/ls85/healthpol031507.asx [hereinafter *Mar. 15, 2007 hearing*].

48. *Mar. 13, 2007 hearing*, *supra* note 47; *Mar. 15, 2007 hearing*, *supra* note 47.

49. *Mar. 13, 2007 hearing*, *supra* note 47; *Mar. 15, 2007 hearing*, *supra* note 47.

50. MINN. STAT. §§ 144.293, subdiv. 8(a), 144.291, subdiv. 2(i) (Supp. 2007).

51. *Id.* § 144.291, subdiv. 2(b).

52. *Id.* § 144.293, subdiv. 8(a).

53. *Id.* § 144.291, subdiv. 2(i).

location.[54] Providers must have a patient's consent to access the information in the RLS.[55] Further, the patient has the right to completely opt-out of the RLS.[56] This right can be exercised when the physician is attempting to get consent to access the RLS.[57] The physician will educate the patient about the RLS and the consent form will have an option to remove the patient and any patient information from the index.[58] However, the patient cannot select which specific records he or she wants in or out of the RLS so the provider will see all RLS entries. The RLS has liability for improper disclosure of information from the RLS.[59]

The MHRA intentionally does not require the creation of one statewide RLS but rather allows as many RLSs as there are HIEs that want to create them.[60] In other words, Hospital A and Hospital B could decide to enter into an HIE and create their own RLS. Other entities like Payer C and Clinic D could create another RLS. In order to deal with multiple patient indices, either providers will need to access multiple RLSs, or a separate RLS that indexes the various indices will be needed.

ii. Representation of Consent

The concept of representation of consent is new to the MHRA. During the legislative hearings for this statute, both the MDH, promoting the law, and the privacy advocates opposing it, looked to Black's Law Dictionary to define a "representation."[61] The first definition is: "A presentation of fact—either by words or conduct—made to induce someone to act . . . ."[62] In the context of the MHRA, a representation of consent allows a physician to obtain consent to access records from a patient and then to simply tell the disclosing provider that the requesting provider has a valid consent.[63] This concept was developed for two reasons: first, to allow

54. *Id.* § 144.293, subdiv. 8(a).
55. *Id.*
56. *Id.* § 144.293, subdiv. 8(d).
57. *Id.*
58. *Mar. 15, 2007 hearing*, *supra* note 47.
59. MINN. STAT. § 144.298, subdiv. 3 (Supp. 2007).
60. *May 1, 2007 hearing*, *supra* note 6.
61. *Id.*
62. BLACK'S LAW DICTIONARY 1327 (8th ed. 2004).
63. MINN. STAT. § 144.293, subdivs. 2(3)–3 (Supp. 2007).

requesting physicians to skip the prior process of faxing consent forms back and forth and, second, to allow requesting physicians to electronically indicate that they have consent so that they can receive the records immediately via an electronic system.[64]

Representation is not an obvious solution to either of the problems noted above. A statutorily adopted universal consent form can resolve the first need.[65] Minnesota now requires the MDH consent form to be accepted as valid consent by all providers.[66] Consequently, the disclosing provider no longer needs to spend time inspecting consent forms for validity. The second problem could be dealt with through an electronic consent process that transmits the actual consent form to the disclosing computer system (once such a system is implemented), as discussed below.

iii. Shared Liability

The MHRA changes the assignment of liability from the prior law, which placed all responsibility for improper disclosure of records on the disclosing physician.[67] The MDH argued that the original liability risk was so large that it created fear of accepting consent forms from another provider and slowed down the exchange of records.[68] Therefore, liability risk has been shifted to whomever the "bad actor" is (the requesting provider, disclosing provider, or the RLS), instead of solely the disclosing physician.[69] Furthermore, the new liability policy complements representation of disclosure by encouraging disclosing physicians to trust that the requesting physicians are truthfully representing that they have valid, signed consent forms. If the disclosing physician discloses, and the requesting physician lies about having consent, then the requesting physician is liable for the disclosure.[70]

64. *Mar. 15, 2007 hearing*, *supra* note 47.

65. MINN. STAT. § 144.292, subdiv. 8 (Supp. 2007). See Minn. Dept. of Health, Minnesota Standard Consent Form to Release Health Information, http://www.health.state.mn.us/divs/hpsc/dap/consent.pdf for the consent form.

66. *See* MINN. STAT. § 144.292, subdiv. 8 (Supp. 2007) ("A form developed by the commissioner must be accepted by a provider as a legally enforceable request under this section.").

67. MINN. STAT. § 144.335, subdiv. 3a(h) (2006).

68. *Mar. 13, 2007 hearing*, *supra* note 47.

69. MINN. STAT. § 144.298 (Supp. 2007).

70. MINN. STAT. § 144.298, subdiv. 2 (Supp. 2007).

This liability shift may be unnecessary because there is now a universal consent form. With the universal consent form, all disclosing providers need to do is to verify that the form appears to be the universal consent form in order to protect themselves from liability as a result of negligence.

III. ANALYSIS: THE MINNESOTA HEALTH RECORDS ACT AS A PUBLIC HEALTH PRIVACY POLICY

The public health community should promote a patient privacy policy for medical records as part of EHR development. Such a policy should include provisions for patient consent, data security standards, and information use regardless of whether the government chooses to build the EHR infrastructure itself or develop a regulatory framework through which private entities act. This section examines the specific provisions of the MHRA and their relation to patient privacy protection. It also analyzes the MHRA as a piece of a larger public health privacy policy.

A. THE PREVIOUS MINNESOTA MEDICAL RECORDS DISCLOSURE LAW WAS A PERCEIVED BARRIER TO IMPLEMENTATION OF ELECTRONIC HEALTH RECORDS

There are two questions central to whether the previous consent law was an impediment to the development of EHRs: first, was there the perception that the law was an impediment, and, second, was the law actually an impediment?

Under the prior Minnesota consent law, consent to disclose medical records generally expired after one year.[71] However, there was an exception to the expiration for disclosure to providers who were being consulted in conjunction with current treatment.[72] "Current treatment" was an undefined term, which gave rise to two competing interpretations of the law.[73] The first interpretation was that a patient had to consent to the release of medical records, but once that consent was made,

71. MINN. STAT. § 144.335, subdiv. 3a(a) (2006).

72. *Id.* § 144.335, subdiv. 3a(c)(1).

73. *See Solutions Report*, *supra* note 2, at 25 ("Some Legal Work Group members argue that as long as the health information exchange is only for patient treatment, then the patient's consent can be fit into this exception. However, other Legal Work Group members argue that, under their interpretation, of 'current treatment' the consent for the RLS would expire in one year.").

medical records could be released to the requesting provider so long as she was currently treating the patient. That means that if Patient X signed the consent form eighteen months prior to coming in with a new problem, the physician could request medical records without a new consent form because she was currently treating the patient. The second interpretation was that the patient must sign a new consent for release of medical records every time the patient was seeking new treatment from a provider. Under that interpretation, the patient consent for release of records was valid for the treatment sought at the time of initial diagnosis, but if the patient returned eighteen months later with a new issue, a new consent for the release of records was needed.[74] The second interpretation is much more restrictive of the release of medical records than the first. The MDH asserted that the differences in interpretations created "irreconcilable differences" between providers regarding proper consent processes.[75] The MDH does not appear to have conducted a study or survey but, instead, relied on the committee opinions that this confusion existed.[76] Nevertheless, it was likely necessary to amend the previous consent law to clarify the process in order to alleviate confusion among providers.

To fully answer the second question—whether the previous consent law actually impeded the development of EHRs—one must understand the prior consent process, the MDH vision for the MHRA consent process, and the consent process as it works today. The MDH explained the prior consent process to the Senate Judiciary Committee.[77] Under the more restrictive interpretation of the prior law, Doctor A determines that Patient X has medical records at another facility from Patient X's statements at Patient X's initial appointment. Patient X signs a consent form for the release of those records. Doctor A faxes the signed consent form to the facility with the records. That facility then inspects the signed consent form to

74. *See id.* at 27–28 (detailing the two interpretations of "current treatment" and the implications on patient consent requirements).

75. *See id.* at 3 ("[T]here are significant and irreconcilable differences in organizations' interpretations of Minnesota's patient consent requirements. These differences make it impossible for health care providers to agree on 'when' and 'how' patient consent is required.").

76. *See generally id.* at 5–7 (describing the background, purpose, and methods of the Minnesota e-Health Initiative).

77. *May 1, 2007 hearing*, *supra* note 6.

determine whether the consent is valid under Minnesota law. If it is valid, the facility releases the records to Doctor A via messenger or mail. If the facility finds the consent lacking, Doctor A drafts a new consent form that meets the disclosing facility's standards and has Patient X sign it. Ultimately, Patient X cannot be treated until the records are at Doctor A's office. Therefore, under this scenario, it is likely that Patient X will need to schedule another appointment to be treated at a time after the records have been received by Doctor A.

The MDH explained its picture of how an EHR health system would work from the patient's perspective.[78] Doctor A determines, from Patient X's statements, that Patient X has medical records at other facilities. Patient X signs a consent form for the RLS, and Doctor A uses the RLS to find the physical location of Patient X's records. Next, Patient X signs a second consent form giving Doctor A permission to access the actual health records from the facilities holding them. Doctor A checks a box in his computer that represents that he has the necessary consent from the patient to view the records he requests. The computer communicates with the computerized database at the other facility (not the RLS) which makes the records available to Doctor A for viewing. All of this would happen in real time, so that Patient X may have his records reviewed during the initial appointment.[79]

Comparing these consent processes, EHR benefits to treatment come from the ability of the requesting and disclosing facilities to exchange records electronically. However, the MHRA does not require interoperable technology; it only changes the consent process to allow for an RLS. It would be perfectly plausible to integrate the technology envisioned in the MDH's description with the consent process of the prior law and without an RLS. Under such a system, Doctor A would still find Patient X's records from Patient X's description (not an RLS) and Patient X would sign a consent form for access to those records. Instead of faxing a consent form to the disclosing facility, Doctor A could send the form to that facility electronically. The disclosing facility would still inspect the form for validity as it did under prior law. Upon finding the consent form valid, the disclosing facility would

78. *See id*.
79. *Id.*

send Doctor A the requested records electronically. Thus, Patient X's records could be reviewed by Doctor A at the initial appointment. Both the modified prior consent process and the envisioned MHRA process would yield health benefits from technology that is not yet widely implemented.

The MHRA consent process with current technology will not yield the health benefits associated with EHRs. Under the MHRA, Doctor A learns from Patient X that there may be records at another facility. Patient X signs a consent form granting Doctor A access to the RLS. Doctor A locates records in the RLS and then requests that Patient X sign another consent form for the release of the specific records Doctor A needs. Patient X signs that consent form. Doctor A calls the facilities holding Patient X's records and represents that he has a valid consent for those records from Patient X. The facility then sends the records over to Doctor A. However, because interoperable technology still has not been implemented, the records are likely messengered or mailed to Doctor A. Therefore, Patient X still must make a second appointment to see Doctor A after the doctor has had a chance to review the records. The MHRA impacts the process described above only up to the point of Patient X's signature on the second consent. The actual exchange of electronic records that is envisioned after that point is a possibility, but not a reality in Minnesota because the necessary interoperable technology has not been designed or implemented.

1. The Prior Consent Law Did Need To Be Revised

Although the prior consent law was not an actual barrier to EHR development, it did need revision because it was a perceived barrier and because it was silent as to the rules for electronic exchange. The electronic exchange of records was not taken into consideration when the previous law was drafted.[80] Therefore, the law did not discuss consent issues surrounding electronic exchange. Because the previous law was silent, there was a larger potential for abuse of electronic exchange where entities could act without any regulation. For example, nothing in the previous law would have prevented the

80. *See Solutions Report*, *supra* note 2, at 3 ("[T]he patient consent requirements were designed for paper-based exchanges of information and early electronic data base systems that are not conducive to real-time, automated electronic exchange of information.").

development of an RLS. The law prohibited the disclosure of health records without patient consent. However, an RLS is an index that simply lists patients' names and the clinics where their records reside. That information was not part of the health record and, thus, could have been collected regardless of the law.[81]

Requiring patient consent to access information in an RLS (or another electronic database) instead of requiring consent for data collection was another necessary development. There are at least four increasingly complex models outlining how electronic exchange could work.[82] Each of these models requires either that EHRs be centrally collected or at least be centrally searchable.[83] Requiring consent from patients to include their records in the system would probably be so time-consuming that the 2015 state mandate for interoperable records would be difficult to meet.[84] However, requiring consent only to access the information still protects patient information while allowing development to move forward. Although this mechanism was unnecessary for an RLS because the RLS does not contain health records, the "opt-out" concept is important for the development and collection of EHRs.[85]

In sum, the previous law was not a structural barrier to the development of EHRs; however, it was necessary to revise the law in some way to resolve disagreement between providers over the consent process and to resolve the perception that it was a barrier. Furthermore, it is preferable for the state to better ensure privacy protection by developing a consent process for EHRs that discourages abuse rather than to remain

---

81. Interestingly, the previous law did not define health records, so whether the RLS would have been legal may have depended upon whether or not the patient's name is considered part of the health record (although it would not be considered part of a health record under HIPAA or the new MHRA). *See* HEALTH INFORMATION SECURITY AND PRIVACY COLLABORATION NATIONAL MEETING, REFORM STATE LAWS RELATED TO THE PRIVACY AND SECURITY OF HEALTH INFORMATION EXCHANGE (Nov. 2007), *available at* http://www.health.state.mn.us/e-health/mpsp/healthrecordsact2007.pdf for a document comparing the old and new law comparing old and new laws.

82. MINNESOTA PRIVACY AND SECURITY PROJECT LEGAL WORK GROUP, CURRENT AND EMERGING MODELS OF HEALTH INFORMATION EXCHANGE: POTENTIAL PRIVACY, SECURITY, AND LEGAL ISSUES (2006), *available at* http://www.health.state.mn.us/e-health/mpsp/legwg/potlegissues071106.pdf.

83. *See id.*

84. *May 1, 2007 hearing*, *supra* note 6.

85. *See supra* notes 56–59 and accompanying text.

silent and allow EHR systems to develop unregulated.

B. PUBLIC HEALTH NEEDS WERE NOT CONSIDERED IN THE MINNESOTA HEALTH RECORDS ACT

There are two potential public health benefits related to EHRs that the MHRA could have developed. First, EHRs could be used for disaster planning and relief during patient relocation.[86] If the MHRA had required the RLS to be able to access the actual EHRs, this public health benefit could have been met. The RLS is not currently available for this use because it is limited to being solely an index of the records' physical location, although it could be developed to allow this use. Second, the RLS could serve a public health function for emergency treatment if it allowed access to a complete list of a patient's records. However, because the law envisions multiple RLSs, the public health benefits of the RLS are greatly reduced. Even if a patient's records were indexed in one RLS, they may not be indexed or may be only partially indexed in the particular RLS to which the provider has access. Furthermore, without the ability to directly access the actual records electronically, the RLS may not reduce the time it takes to access the needed records once they have been located.

The other large public health need for EHRs is related to research.[87] The MHRA did not, and was not intended to, create a public health database that would allow researchers to access de-identified aggregate data. Again the RLS could develop into a system that allows such research but the MHRA did not envision it. Ultimately, public health uses of EHRs were not considered under the MHRA.

Individual privacy protection was considered by the drafters of the MHRA, at least insofar as individuals can consent to record disclosure. However, public health privacy protections require a broader privacy policy that encompasses data security and control over use of information. Public health should be particularly concerned with policies regarding appropriate information use because of the potential for data misuse to have broad social consequences. The MHRA does not discuss appropriate data use at all. While it clearly outlaws dissemination of records, it places no limits on providers' access

86. *See supra* notes 19–20 and accompanying text.

87. *See supra* note 23 and accompanying text.

to the RLS index once a patient consents to it. Notably, the MHRA does not limit providers' access to the RLS for treatment purposes. Arguably, the administrative and marketing arm of a provider network (which would still be a "provider" under the statute) could access the RLS once consent is given and mine the index for data about patient traffic between the provider and its competitors. There is no law or policy allowing, disallowing, or regulating this kind of data use.

For some particular public health endeavors, such as mental health, drug treatment, and family planning, confidentiality is especially important. Patients who do not feel that these records are kept confidential may not seek treatment at all.[88] The MHRA does not allow patients to shield specific providers they have visited from the RLS. Thus, patients have the choice to either participate fully in the RLS or not participate at all. Patients who wish to keep certain visits confidential will either choose to not participate in the RLS (which has one set of undesirable public health consequences) or will choose not to seek treatment (which can also have adverse public health consequences). Ultimately this dilemma is untenable for public health. If the MHRA had considered these problems it could have required the RLS to allow individuals to selectively shield specific information from it. That policy would have respected the individual's autonomy and right to control access to their records while also avoiding the potential repercussions explained above.

88. There may be state consent laws related to these particularly sensitive areas that prevent the inclusion of these records in the RLS, but specific exclusions are not contemplated by the MHRS. *See e.g.* Mental Health: A Report from the Surgeon General, http://www.surgeongeneral.gov/library/mentalhealth/chapter1/sec1.html#approach (last visited Dec. 11, 2008)(discussing the stigma associated with mental illness, and the impact that stigma has on seeking treatment). The logical conclusion is publicizing and individual's treatment may make him or her less likely to seek it to begin with. Similar arguments can be made for both drug treatment and family planning decisions. *See e.g.* U.S. Dep't of Health & Human Services, Alcohol and Drug Information, http://ncadi.samhsa.gov/govpubs/bkd107/2f17.aspx (last visited Dec. 11, 2008) (noting that one impact of required reporting laws is that women may forego care).

C. THE MINNESOTA HEALTH RECORDS ACT DOES NOT BALANCE INDIVIDUAL PRIVACY WITH ELECTRONIC HEALTH RECORD DEVELOPMENT

The MHRA does not balance individual privacy with EHR development because the law neither inhibits nor encourages EHR development. The MHRA itself does not create an EHR system. The real benefit of instant access to EHRs will come when health records are actually exchanged electronically. Neither electronic transmission of consent nor electronic disclosure of records is required by the MHRA, and the technologies needed to complete these steps have not yet been implemented. Thus, the MHRA does not create an EHR system.

Furthermore, the electronic provisions in the MHRA are specifically tailored to the development of an RLS, which may or may not be useful in the ultimate EHR system. The RLS could develop into a system that allows a physician, with the proper consent, to access records at another facility electronically. But it is equally likely that the state will develop a different infrastructure where the RLS is irrelevant to the electronic exchange of information. The concept is further confused by the fact that the MDH intends for there to be multiple RLSs.[89] Consequently, even if an RLS is useful for one HIE, a broader RLS would have to be created to search all of the other RLSs before this approach would work as a statewide system.

The MHRA is concerned with individual privacy, but the law neither strengthens nor weakens privacy protections as compared to the prior consent law. The fact that an individual cannot shield specific information from the RLS is a glaring privacy problem. However, the MHRA requires the patient to consent twice to providers' access to records before a physician can view them, whereas the previous law required the patient's consent only once.[90] This added consent requirement may provide more privacy protection even as it slows down a provider's access to patient records. It is impossible to assess whether the MHRA will provide sufficient privacy protection in an EHR system because the other components of a privacy policy, data security and information use, have not yet been

89. *May 1, 2007 hearing*, *supra* note 6.

90. *See supra* notes 71–76 and accompanying text.

developed. The MDH might argue that the MHRA is one small piece of a much larger EHR and privacy picture and that this law, while not directly creating EHRs, removes at least one barrier to development. The problem is that the rest of the picture is still so vague and unknown that it is difficult to know whether this law will be congruent with the entire scheme or will need another revision.

D. SPECIFIC PROVISIONS OF THE MINNESOTA HEALTH RECORDS ACT SHOULD BE AMENDED

1. The Record Locator Service

The RLS provisions have two significant problems. First, the RLS does not allow individuals to shield specific information and, second, the MHRA allows multiple RLSs to develop. Privacy advocates objected to the RLS, testifying that even without medical records, the RLS may expose significant patient information to a large number of people.[91] The term "provider" is not limited to a care giver but may extend to the administrative arm of a hospital or clinic.[92] Therefore individuals that are not caregivers may be accessing the information in the RLS. Also, the RLS may reveal significant medical information simply by listing the clinic or physician that the patient visited. For example, if the RLS lists that records are located at Planned Parenthood, the individual accessing the RLS may draw conclusions about the patient's sexual activity or family planning decisions. A policy that both allows patients to remove specific information about themselves from the RLS and controls how RLS information can be used would limit this privacy threat.

Privacy advocates further argued that a physician might learn information about a patient that are not related to the physician's treatment of that patient.[93] The patient may not understand the implications of withholding certain information from the RLS. For example, a patient may think that a dentist does not need to know about the patient's cancer history because the dentist is only treating the teeth. A dentist might

---

91. *See, e.g.*, *Mar. 13, 2007 hearing*, *supra* note 47.

92. *See* MINN. STAT. § 144.291, subdiv. 2(h) (Supp. 2007)(the definition explicitly includes a licensed health care facility, which could have many non-licensed professionals accessing information for administrative reasons).

93. *See* sources cited *supra* notes 38–39.

examine a patient more carefully or change prescriptions or treatment plans if the dentist knows that the patient is also being treated for cancer. Furthermore, a physician is prohibited from disclosing medical information in the RLS without consent by both the MHRA and the state licensing standards.[94] Nevertheless, the patient should have ultimate control over any disclosure of her medical records. Yet the system, as it is currently envisioned, limits the patient's choice to either opting entirely in or entirely out of the RLSs.

The fact that the MHRA allows for multiple RLSs to be developed seriously limits the utility of the system because a patient's records might be indexed in several RLSs and there is no provision for a single master index covering all RLSs. Further, because these RLSs are owned and operated by an HIE, they will be funded by the health care entities in the HIE. Presumably, charges to the patient will ultimately fund the operation of an RLS. Given that there will be many RLSs and a hospital might have to belong to many of them to get a complete picture of its patients' records, these costs will be driven up unnecessarily. A cleaner solution is simply to create a central RLS.

2. Representation of Consent

Privacy advocates objected to the representation of consent because they felt that made it too easy for an individual to lie in order to access records. In other words, insurers or employers could simply present themselves as a provider with consent and have records released to them. This argument is weak because even without the concept of representation, an individual interested in obtaining medical records can manufacture a paper consent and fax it to a physician. Basically, an individual intent on stealing specific records can lie and do so regardless of the consent process.

Two electronic solutions were suggested at the hearings: (1) using electronic signatures or (2) using electronic pads similar to those used at grocery stores for credit card validation.[95] It is unclear why neither of these options was adopted in the final bill, and the MDH did not offer a reason at the hearings. There are three advantages to these solutions:

94. MINN. STAT. § 147.091, subdivs. 1(o, m) (Supp. 2007).

95. *May 1, 2007 hearing*, *supra* note 7.

(1) they would eliminate the need for providers to keep paper consent forms; (2) they would remove the perception that the MHRA weakens patient privacy protection in order to promote EHR development; and (3) they would strengthen privacy protection because a "bad actor" would have to hack into a closed system, manufacture the signature, and relay it to the disclosing computer system. Currently, a "bad actor" would have to print the universal consent form from the MDH webpage, forge a patient's signature on it, and fax it to the disclosing office. This approach requires much less expertise than hacking into a sophisticated and secure database system.

The representation of consent is an unsatisfactory device to promote information exchange because it increases the perception that patient consent is weakened while, at the same time, it fails to provide the greater security protections inherent in an electronic consent process. An electronic consent process should be developed and implemented and the representation of consent repealed.

E. THE MINNESOTA HEALTH RECORDS ACT AS PART OF A BROAD PRIVACY POLICY

From a public health perspective, the MHRA does not provide a satisfactory privacy policy for EHRs. Such a policy should include consent, data security requirements, and controls over information use. Regulations in each of these three areas must be coordinated with one another because the requirements of one section may affect the requirements of the others. The MHRA deals only with the consent issue, not with the other two areas of concern. It is likely that the MHRA will have to be revised again when those areas have been developed and when it becomes clear whether the RLS will be part of Minnesota's EHR system.

In one significant way, the MHRA may actually inhibit further privacy policy development. The RLS is run by private non-governmental entities that make money operating it. These RLSs will now be stakeholders in any further EHR development and will have an interest in maintaining the RLS whether or not the RLS is a logical electronic component for the EHR system. Furthermore, these stakeholders will probably be interested in maintaining private development of the electronic infrastructure which could block the government from developing a universal system that would promote public

health interests.

In sum, the MHRA should be amended to allow individuals to shield specific information from the RLS, to create one central RLS rather than allowing for the development of multiple RSLs, and to develop an electronic consent process to replace the representation of consent. Finally, the MHRA may have to be further altered as regulations for data security standards and control over data use are developed. Without those pieces, it is impossible to know whether the RLS consent requirements provide sufficient privacy protection for EHRs.

IV. CONCLUSION

The benefits of EHRs for efficiency in treatment alone are great enough that health care companies will continue to move away from paper records. The benefits in individual care and public health are of a great enough social benefit to justify a public policy supporting a shift to EHRs. Patient privacy protection is integral to the public health benefits of EHRs because, without it, data collected through EHR networks may be unreliable. Furthermore, the ease with which entire bodies of electronic records can be disseminated en masse and the ability to mine that data in unforeseen ways poses a heightened threat to individual privacy if the data were used inappropriately. Patient consent to dissemination of records may produce unintended and possibly adverse consequences in large part because we cannot yet foresee the entire impact of EHRs on individual health care and public health. Therefore, patient consent, while still a necessary component of privacy protection in an electronic era, is not a sufficient protection by itself.

Public health agencies should advocate for privacy policies that will adequately protect patients because a lack of regulation will allow for information misuse to occur. To adequately protect privacy, laws supporting EHR technology need to include regulations covering at least the following areas: (1) patient consent to the release of medical records; (2) state-of-the-art data security for electronic systems; and (3) acceptable data use, including any sale of information that is illegally obtained from the EHR system. Regulations in all three areas need to be developed simultaneously because it is difficult to know how to adequately regulate one area without some sense of how the other two areas will be handled. For

example, it is difficult to develop a patient consent law without knowing what the data security requirements will be, for the data security may impact both the kind of patient consent required and the point at which the patient should give it.

The MHRA was portrayed in the media as a major step toward the development of EHR technology in Minnesota. The e-health committee publications maintained that the MHRA strengthened rather than weakened privacy protection. The MHRA does not necessarily move Minnesota towards e-health. The electronic innovations in the law are limited to an RLS that is only an electronic index of the physical locations of records. That index could be used in the final EHR system, but it is equally likely that it will not be. As an individual privacy policy, the MHRA is neither more nor less protective of individual privacy than the prior law was, nor is it more or less burdensome. The MHRA requires two consent forms instead of one to access records, but as it will be used today a patient may still have to make a separate appointment to be treated on the basis of outside records. The MHRA simply creates a different consent process than the prior consent law did. The MHRA should, however, be amended in at least three ways: 1) to allow individuals to shield specific information from the RLS, 2) to require the creation of one central RLS, and 3) to replace the representation of consent with an electronic consent process. These changes would strengthen privacy protections and better meet public health purposes.

As a public health privacy policy, the MHRA is not sufficient. The MHRA focuses narrowly on the patient consent process for records disclosure, and thus only deals with one of the three interdependent public health privacy components. Because the other two components, data security standards and data use, are not yet developed, it is impossible to determine whether the MHRA will provide a sufficient consent process for the future electronic health record system. It is likely that the MHRA will be revised again once EHRs have been more fully developed.