ANNALS OF HEALTH LAW
Advance Directive

VOLUME 23 SPRING 2014 PAGES 153-163

Ready or Not, Here They Come: A Discussion of the Legal and Ethical Considerations for the Implementation of Electronic Medical Records

Ashley R. Huntington[*]

I. INTRODUCTION

Perhaps the oldest known principle in medical ethics is "do no harm."[1] While short and sweet, this axiom is loaded with difficult questions, especially in an era of great medical innovation.[2] Despite the momentous innovation and evolution of health care, many medical providers must approach patients who have untreatable and terminal illnesses and give them options that are experimental and may ultimately cause harm, or choose to do nothing, which results in certain harm.[3] Because of this array of choices, medicine has moved away from the simplicity of "do no harm," and moved into a more nuanced idea of choosing one care plan that is no more harmful than any other care plan.[4] However, many medical providers do not take into consideration the idea that "do no harm" applies much more broadly—this axiom should be followed when using, accessing, and disclosing a patient's personal health information (PHI). Attention to the security of a patient's PHI is more important than ever, especially as an increasing number of medical providers are making the transition from paper medical records to

[*] Juris Doctor Candidate, Loyola University Chicago School of Law, Class of 2015. Ms. Huntington is a staff member of *Annals of Health Law*.

[1] Scott Groudine & Philip D. Lumb, *First, Do No Harm*, 23 J. MED. ETHICS 377, 377 (1997).

[2] *Id.*

[3] *Id.*

[4] *Id.*

electronic medical records (EMRs).[5] Although significant concerns surround the implementation of EMRs, especially with regard to data security, this article will argue that the implementation and effective use of EMRs allows medical providers to facilitate the best care for their patients as long as proper safeguards for data security are in place first. Part I of this article will explore the advantages of EMRs and how they allow medical providers to give the best care to their patients. Part II will delve into the criticisms and concerns about EMRs, specifically about data security. Part III will show that through a successful and well-planned pre-implementation phase, EMRs that have the required safeguards, technical support, and other factors will allow the system to produce more beneficial and ethical care.

II. A REVIEW OF THE LEGAL AND ETHICAL INCENTIVES OF EMR IMPLEMENTATION

Although the widespread implementation of EMRs across the healthcare field draws significant concerns from medical providers, as well as patients, using such records also has important legal, ethical, financial, and health benefits that justify their implementation.[6] Even though the technology for EMRs dates back to the 1970s, the push for implementing such technology is a relatively recent trend.[7] In 2004, former President Bush set the goal for a majority of Americans to have an EMR within ten years.[8] Current statistics for implementation show that in 2012, seventy-two percent of office-

[5] *See* CHUN-JU HSIAO & ESTHER HING, CTR. FOR DISEASE CONTROL AND PREVENTION, USE AND CHARACTERISTICS OF ELECTRONIC HEALTH RECORD SYSTEMS AMONG OFFICE-BASED PHYSICIAN PRACTICES: UNITED STATES, 2001-2012, at 1 (2012), *available at* http://www.cdc.gov/nchs/data/databriefs/db111.pdf. The percentage of office-based physicians using EMR systems increased from forty-eight percent in 2009, to seventy-two percent in 2012, with individual state implementation ranging from fifty-four percent in New Jersey to eighty-nine percent in Massachusetts. *Id.*

[6] *See generally* Richard Hillestad et al., *Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, and Costs*, 24 HEALTH AFFAIRS 1103 (2005).

[7] Karoline Kreuser, *The Adoption of Electronic Health Records*, 16 ANNALS HEALTH L. 317, 318 (2007).

[8] *Id.*

based physicians used EMR systems,[9] while a little over forty-four percent of hospitals used at least a basic EMR system in 2012.[10]

This dramatic increase in EMR implementation seems to be motived at least partially by the Health Information Technology for Economic and Clinical Health Act (HITECH) and the American Recovery and Reinvestment Act (ARRA), which provide incentives to eligible professionals and eligible hospitals that participate in Medicare and Medicaid programs, and that are meaningful users of certified EMR technology.[11] Under the incentive programs, eligible professionals can receive up to $44,000 through the Medicare incentive program, and up to $63,750 through the Medicaid incentive program, with payments totaling up to an unprecedented $27 billion over ten years.[12] Although these incentives may not be enough to cover the entire cost of an expensive EMR system implementation, the incentives can help to defray some of the cost, which will make implementation less burdensome for smaller practices.[13] Central to the incentive programs is the demonstration of meaningful use of EMR systems, which is divided between a set of core objectives and a menu of ten additional tasks.[14] Provid-

[9] HSIAO & HING, *supra* note 5.

[10] *See* OFF. OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., *Adoption of Electronic Health Record Systems Among U.S. Non-Federal Acute Care Hospitals, 2008-2012*, *available at* http://www.healthit.gov/sites/default/files/oncdatabrief9final.pdf.
Hospital adoption of EMR systems more than tripled since 2009, when only twelve percent of hospitals had and used a basic EMR system. *Id.*

[11] *Electronic Health Record Medicaid Incentive Payment Program (eMIPP)*, ILLINOIS DEP'T OF HEALTHCARE AND FAM. SERVS., http://www2.illinois.gov/hfs/MedicalProvider/eMIPP/Pages/default.aspx (last visited
Apr. 5, 2014). The incentive program is designed to encourage eligible professionals and eligible hospitals to adopt, implement, or upgrade certified EMR technology and use it in a meaningful manner—the program is not designed to serve as a reimbursement. *Id.*

[12] *EHR Incentive Programs*, CMS.GOV., https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/ehrincentiveprograms/ (last visited Apr. 5, 2014). Eligible hospitals are eligible to receive payments from both incentive programs, while eligible professionals are only able to receive payments through one incentive program of their choosing. *Id*. Differences between the programs include the time period over which payments are made, the agency running the program, payment adjustments, and the degree to which meaningful use must be demonstrated. *Id.*

[13] *Id.*

[14] David Blumenthal, *The "Meaningful Use" Regulation for Electronic Health Rec-*

ers can choose any five off this menu to implement, thus giving them autonomy in deciding their own path toward full EMR implementation.[15] The meaningful use rule creates a balance between the importance of adopting EMRs while still recognizing the risks and challenges that are associated with such implementation.[16]

In addition to the legal incentives that accompany the implementation of an EMR system, it has a number of ethical advantages.[17] EMRs are generally seen as a way to achieve quality and continuity in treatment while also being cost effective.[18] At the most basic level, EMRs can provide medical providers with ready access to a patient's complete lifetime medical history.[19] EMRs provide increased accessibility of a patient's medical history for medical providers and make it possible for medical providers to make the best choices for care after reviewing the more complete medical history provided by an EMR[20], thus allowing them to "do no harm."

The ability to review a complete medical history and make decisions based on that history is especially important if a medical provider is participating in an Accountable Care Organization (ACO). An ACO is a group of doctors, hospitals, and other healthcare providers who come together voluntarily to give coordinated, high-quality care to Medicare patients.[21] Although participation in an ACO is completely voluntary for medical providers, incentives are available when providers keep costs down and meet specific benchmarks, focusing on prevention and carefully managing pa-

ords, 363 NEW ENG. J. MED. 501, (Aug. 5, 2010), *available at* http://www.nejm.org/doi/full/10.1056/NEJMp1006114.

[15] *Id.*

[16] *Id.*

[17] *See* Wes Fisher, *Patient Safety and the Ethics of EMR Implementation*, MEDPAGE TODAY (Jan. 22, 2013), http://www.medpagetoday.com/DrWes/36939.

[18] Kreuser, *supra* note 7, at 319.

[19] *Id.*

[20] *Id.*

[21] *Accountable Care Organizations (ACO),* CTRS. FOR MEDICARE & MEDICAID SERVS., http://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/ACO/ (last visited Apr. 5, 2014).

tients with chronic diseases.[22] Thus, providers receive more compensation for ensuring that their patients remain healthy and out of the hospital.[23] EMRs can help facilitate this quality care.[24]

EMRs have the capability to provide diagnostic and treatment advice while allowing the medical provider to make the final decision for course of care.[25] EMRs have the ability to track when a clinician ignores a warning or advice, especially for potentially dangerous medication interactions, thus providing enhanced accountability for care.[26] However, it should be noted that many medical decisions cannot be made on entirely scientific or computer-based grounds[27] because providers must consider all aspects of care, including the underlying goals and values of the individual patient.[28]

III. Data Security and Other Concerns Surrounding EMR Implementation

As previously noted, opponents of EMRs have a number of fears about the widespread implementation of EMRs, especially with regard to data security issues. This section will discuss the opposition to EMRs, but ultimately show that the main concern of data security can be taken into consideration and remedied before implementation takes place. A quick review of newspaper headlines from the past few years reveals an increasingly significant problem for consumers in the United States: data security. While credit card and identity information can be valuable to thieves and hackers, what many consumers and medical providers fail to realize is that health information is significantly more valuable, thus making it highly sought-

[22] *Id.*

[23] Jenny Gold, *Accountable Care Organizations, Explained*, NPR, (Jan. 18, 2011, 8:21 AM), http://www.npr.org/2011/04/01/132937232/accountable-care-organizations-explained.

[24] *See generally* Hillestad, *supra* note 7, at 1106.

[25] *See* Peter S. Winkelstein, *Ethical and Social Challenges of Electronic Health Information*, *in* MED. INFORMATICS,139, 147 (Hsinchun Chen et al. eds., 2005).

[26] *Id.*

[27] *Id.*

[28] *Id.*

after.[29] Because of PHI's value, cases involving hospital personnel selling PHI are occurring more than ever.[30] But as more medical providers transition to EMRs, the risks of data breaches and unauthorized PHI disclosures may seem greater because EMRs allow more individuals access to patient records.[31] These risks make some patients resistant to having their PHI stored on EMRs.[32] Among the most serious effects of a data breach are the patient's loss of health insurance or the patient being held financially accountable for medical expenses related to treatments they did not receive,[33] however some breaches ultimately have little consequence on the patients affected.[34]

Though the value of electronic records is particularly worrisome for patients, medical providers should be concerned with ensuring the security of electronic records because of the serious legal consequences that come with lack of data security, specifically under the Health Insurance Portability and Accountability Act (HIPAA).[35] HIPAA provides both civil and criminal

[29] *See* Jim Avila & Serena Marshall, *Your Medical Records May Not Be Private: ABC News Investigation*, ABC NEWS, http://abcnews.go.com/Health/medical-records-private-abc-news-investigation/story?id=17228986&singlePage=true (last visited Apr. 5, 2014). Thieves may approach medical staff and offer upward of $500 per week for providing twenty to twenty-five insurance claim forms, medical records, or health financing records. *Id.*

[30] *See* NITROSECURITY & FAIR WARNING, SECURITY AND PRIVACY OF ELECTRONIC MEDICAL RECORDS 4 (2011), *available at* http://www.himss.org/files/HIMSSorg/content/files/SecurityandPrivacyofElectronicMedicalRecords.pdf.

A Howard University hospital medical technician pleaded guilty to selling patient information, including names, birth dates, and Medicare numbers, for $500 to $800 per transaction for over a year. *Id*. An admissions clerk at the Baptist Health Medical Center in Little Rock, AR was recently accused of using stolen patient information to buy Wal-Mart gift cards. Approximately 1,800 patient records were exposed. *Id.*

[31] *See* Judy Foreman, *At Risk of Exposure*, L.A. TIMES (June 26, 2006), http://articles.latimes.com/2006/jun/26/health/he-privacy26. One report estimates that at least 150 people, including nurses, x-ray technicians, and billing clerks have access to at least part of a patient's records during hospitalization. *Id.*

[32] *See* Maranda Gibson, EMRs Cause Concern Among Patients, SIGNAL NEWS (Mar. 1, 2011), http://signalnews.com/emrs-cause-concern-among-patients.

[33] Peter P. Yu, *Ethical Principles and the Use of Electronic Health Records*, ASCO DAILY NEWS (June 1, 2013), http://am.asco.org/ethical-principles-and-use-electronic-health-records.

[34] *Id.*

[35] *See*, *HIPAA Violations and Enforcement*, AMA, http://www.ama-assn.org//ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/

penalties based on the number of violations and degree of knowledge involved in a breach.[36] Aside from civil and criminal penalties, entities involved in a breach are also required to provide individual notices to those affected by the breach, and must notify the media if the breach impacts over 500 individuals.[37]

Aside from the legal considerations involved with potential data breaches and the security of PHI, medical providers should consider the ethical implications that come with a transition to EMRs. These considerations include the continued obligation to keep their patients' information safe, while making the best decisions for their patients' care.[38] Because EMRs come with enhanced portability and accessibility, ethical questions are raised with regard to medical providers informing their patients of the potential for privacy breaches.[39] These questions include whether patients must be informed that EMR vendors sold, or have the rights to sell, de-identified copies of patient databases to pharmaceutical companies, medical devicemakers, and health services researchers.[40]

Additionally, the technology of many EMR systems allows them to provide automatic alerts such as dangerous drug interactions and suggestions for treatment and diagnosis.[41] While these warnings and suggestions can be viewed as merely advice, the availability of such technology raises ethical

hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page (last visited Apr. 5, 2014). Under HIPAA's civil penalties, entities may be fined between $100-$50,000 per violation, or up to $1.5 million in a calendar year. *Id*. Individuals may receive between one and ten years in prison if criminal liability is found under HIPAA. *Id.*

[36] *Id.*

[37] *Breach Notification Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/ (last visited Apr. 5, 2014).

[38] Dean F. Sittig & Hardeep Singh, *Legal, Ethical, and Financial Dilemmas in Electronic Health Record Adoption and Use*, 127 PEDIATRICS e1042, e1044 (2011).

[39] *Id.*

[40] EMR vendors such as Cerner, GE, and Allscripts [formerly Eclipsys] have all sold de-identified patient information to a variety of health care companies. *Id.* EMRs may also be used for quality reviews, administrative reviews, and utilization studies to manage the business aspects of health care. Kreuser, supra note 7, at 320.

[41] Winkelstein, *supra* note 26, at 146.

questions about whether the provider or the computer is ultimately making treatment decisions.[42] Medical providers must remember that computer technology can be prone to errors, crashes, and other unavoidable accidents, and thus must exercise sound judgment aside from computer recommendations when engaging in clinical decision-making.[43] Further, by shifting to centralized record-keeping through EMRs, patients are able to receive periodic or on-demand reports of the audit trail of accesses to their records.[44] These reports can then lead to the assumption that the patient is responsible for monitoring their medical reports much like they are responsible for monitoring their credit card statements.[45]

IV. COMBATING DATA SECURITY ISSUES THROUGH PRE-IMPLEMENTATION PLANNING AND POST-IMPLEMENTATION SUPPORT

Although concerns surrounding EMRs range from data security issues to allowing technology to take over the medical provider's role in making decisions for patient care, many of these issues can be avoided with proper EMR implementation.[46] At the center of successful implementation are three factors: people, process, and technology.[47] Generally, three main phases will occur during implementations: pre-implementation, implementation, and post-implementation.[48] It is important to note that the three main factors may exist in all stages of implementation, or many only exist in a single stage of implementation.[49] Perhaps most important to the successful

[42] *Id.* at 146–47.

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] *See* Karim Keshavjee et al., *Best Practices in EMR Implementation: A Systematic Review* 1, 3 (2006), *available at* http://www.infoclin.ca/assets/7e474_best%20practices%20in%20emr%20implementation%20-%20july,%202006.pdf.

[47] *Id.*

[48] *Id.*

[49] *Id.* For example, provider governance, EMR project leadership, and project stakeholders will be involved in all stages of implementation, though tasks such as choosing software and work-flow redesign will only be involved in the pre-implementation and implementation phases, respectively. *Id.* at 4.

implementation of an EMR system is the pre-implementation phase, where project managers decide the mission and vision for the system, where software is chosen, and where project managers sell the benefits of the system to personnel.[50] During the actual implementation of the EMR, it is critical that the EMR functions and usability align with the workflow of physicians and staff.[51] Further, training for the EMR system must take place during implementation and should be on-going so as to facilitate a smooth transition to paperless patient care.[52] Finally, post-implementation technical support and incentives are important for maintaining the EMR system and ensuring that users are utilizing it properly.[53]

In addition to ensuring strong pre-implementation planning and post-implementation support, biometric authentication offers another solution to the problem of data security of EMRs.[54] Biometric authentication is generally seen as more advantageous compared to token-based or knowledge-based systems.[55] It has been suggested that to allow the maximum availability of records to both patients and medical providers, a combination of signature and voice recognition should be implemented into EMR systems.[56]

V. CONCLUSION

In an age of rapidly growing medical technology, it is inevitable that EMRs will be implemented, but the key to successful implementation in-

[50] *Id.* at 4. Ensuring internal readiness for an EMR system has been shown to be important in the successful implementation of EMRs. *Id.* EMRs bring serious changes to an organization, so it become essential to demonstrate the benefits of the system to physicians, nurses, and staff while addressing possible obstacles and barriers. *Id.*

[51] *Id.* at 7.

[52] *Id.*

[53] *See id.* at 8.

[54] *See* Stephen Krawczyk & Anil Jain, *Securing Electronic Medical Records Using Biometric Authentication*, in AUDIO- AND VIDEO-BASED BIOMETRIC PERSON AUTHENTICATION, 1, 2 (Kanade et. al eds., 2005).

[55] *Id.* at 2. Biometric authentication can include systems that use modalities such as fingerprints, iris scanning, signatures, or voice recognition while token-based authentication refers to the usage of identification cards, and knowledge-based authentication refers to password systems. *Id.*

[56] *Id.* at 3.

volves three stages and many factors.[57] Critics of EMRs cite numerous concerns of data security, an increased likelihood for data breaches, and the possibility that EMRs may take over medical providers' job of diagnosing.[58] However, the benefits of EMRs outweigh the negatives.[59] Not only do medical providers have financial incentives through HITECH and ARRA, but using EMRs allows medical providers to provide better care and communicate more effectively with other clinicians, as well as patients. These benefits relate back to the central ethical goal in medicine of "do no harm." By utilizing the available EMR technology, medical providers put their patients' care first, and they are able to see a complete medical history before making any decisions about course of care.[60] The complete implementation of EMRs is no longer a possibility, but rather a process that is occurring rapidly in an effort to bring patient health records into the twenty-first century.[61] While clinical alerting and decision-making systems can improve the quality of health care for patients, it is essential that these systems are implemented properly.[62] By following the three stages of implementation, and paying special attention to the pre-implementation phase, EMRs have the possibility to make healthcare easier and more accessible.[63] Ongoing attention to EMR systems, which includes providing EMR users with training and education about the abilities and limitations of the system, as well as evaluating and maintaining systems, is critically important.[64] Using biometric authentication is another way to help combat the problem of data se-

[57] *See* Keshavjee et al., *supra* note 47, at 3.

[58] *See* Winkelstein, *supra* note 26, at 147.

[59] *The Benefits of EHRs Drastically Outweigh the Risk*, EXSCRIBE (Oct. 14, 2013), http://www.exscribe.com/orthopedic-e-news/ehremr/the-benefits-of-ehrs-drastically-outweigh-the-risks.

[60] Kreuser, *supra* note 7, at 319.

[61] *See* David Blumenthal, *The Future of Health Care and Electronic Records*, HEALTH IT BUZZ (July 13, 2010, 4:11 PM), http://www.healthit.gov/providers-professionals/benefits-electronic-health-records-ehrs.

[62] *See* Winkelstein, *supra* note 26, at 149.

[63] *See* Keshavjee et al., *supra* note 47, at 3.

[64] *See id.* at 7-8.

curity with EMRs.[65] Both voice recognition and signature verification can allow maximum access to both patients and medical providers while still being less invasive than fingerprint or iris scanning.[66] Further, medical providers must remember the ethics of their profession and strive to understand the advice produced by EMR systems while still choosing care actions based upon the patient's values and the goals of their health care.

[65] *See* Krawczyk & Jain, *supra* note 55, at 3.

[66] *Id.*