2010

Employing E-Health: The Impact of Electronic Health Records on the Workplace

Sharona Hoffman
Case Western Reserve University School of Law, sharona.hoffman@case.edu

EMPLOYING E-HEALTH: THE IMPACT OF ELECTRONIC HEALTH RECORDS ON THE WORKPLACE

Sharona Hoffman[*]

INTRODUCTION

Electronic Health Record (EHR) systems may soon become a fixture in most medical settings. The Obama administration, like the Bush administration before it, has stated that its goal is to computerize all Americans' health records by 2014.[1] President Obama's stimulus plan, passed in response to the current recession, includes $19 billion for the promotion of health information technology.[2] EHR systems are likely to change medical practice in the United States significantly and have the potential to improve health outcomes.[3] However, their impact will not be restricted to health care. This Article explores how the advent of EHRs will affect the American workplace.

Employers may obtain and process EHRs for a variety of reasons. Many require applicants who have received employment offers to provide authorizations for release of medical records in order to verify the individuals' fitness for duty.[4] At times, employers require records for purposes of workers'

---

* Professor of Law and Bioethics, Co-Director of the Law-Medicine Center, Case Western Reserve University School of Law. B.A., Wellesley College; J.D., Harvard Law School; LL.M. in Health Law, University of Houston. The author would like to thank Andy Podgurski and Jonathan Entin for their helpful comments on previous drafts.

1. *See* American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, Title XIII. § 3001(c)(3)(A)(ii), 123 Stat. 115, 231 (2009) (to be codified at 42 U.S.C. § 300jj-11(c)(3)(A)(ii)).

2. David Blumenthal, *Stimulating the Adoption of Health Information Technology*, 360 NEW ENG. J. MED. 1477, 1477 (2009).

3. *See generally* Sharona Hoffman & Andy Podgurski, *Finding A Cure: The Case for Regulation and Oversight of Electronic Health Record Systems*, 22 HARV. J.L. & TECH. 103, 112-126 (2008) (discussing the benefits and risks of EHR systems).

4. *See* Americans with Disabilities Act (ADA), 42 U.S.C. § 12112(d)(3) (2006) (authorizing employers to require medical examinations after an offer of employment has been made and prior to the commencement of employment); Mark A. Rothstein, *Is GINA Worth the Wait?*, 36 J.L. MED. & ETHICS 174, 177 (2008) (stating that each year over 10 million authorizations for release of medical information are signed by individuals who have received conditional job offers).

compensation claims, reasonable accommodation requests by individuals with disabilities, or Family Medical Leave Act (FMLA) requests.[5] Employers who are self-insured also process employees' medical data in order to pay insurance claims.[6]

EHR systems raise a variety of concerns for both employees and employers. The existence of voluminous electronic records may make the handling of medical data far more cumbersome and complicated for employers. The availability of comprehensive, integrated EHRs may also raise workers' concerns that employers will obtain personal health details and use them as the basis for discriminatory decisions. Computerization and the security vulnerabilities of electronic systems may also introduce new privacy threats for applicants and employees and new worries about privacy breaches and associated litigation for employers.

Employers provide approximately sixty percent of Americans with health care coverage,[7] and they are therefore strongly affected by health care costs. In the long term, EHR systems may save costs through their efficiencies and sophisticated technological abilities.[8] In the short term, however, medical practices must absorb the cost of purchasing and implementing EHR systems, and poorly trained operators or product defects may generate increased medical errors.[9] In addition, some commentators argue that automation will enhance billing opportunities for providers and increase charges.[10]

EHRs will also impact workplace litigation involving medical data. EHRs may be more difficult than paper records to produce and review.

---

5. Cynthia Nance et. al., *Discrimination in Employment on the Basis of Genetics: Proceedings of the 2002 Annual Meeting, Association of American Law Schools Section on Employment Discrimination Law*, 6 EMP. RTS. & EMP. POL'Y. J. 57, 71 (2002); 29 U.S.C. § 2613(b)(3) (2006) (requiring certification from a health care provider for purposes of FMLA requests that includes "the appropriate medical facts within the knowledge of the health care provider regarding the condition"); 42 U.S.C. § 12112(d)(3)(B)(i) (allowing release of medical information to supervisors and managers for purposes of reasonable accommodation); ALA. CODE § 25-5-77(b) (2009) (addressing disclosure of information to employers for workers' compensation purposes); MINN. STAT. ANN § 363A.20 Subd. 8(2) (West 2009) (addressing the release of medical information for a variety of reasons); OHIO REV. CODE ANN. § 4123.651(B) (West 2009) (addressing medical information release forms for workers' compensation claims).

6. Surveys by the Kaiser Family Foundation and Health Research and Educational Trust found that 55 percent of workers with health benefits were covered by self-insured plans in 2007, up from 44 percent in 2007. Emily Berry, *Who's Behind the Card? Plans Sometimes Administer, Rather than Insure*, AMEDNEWS.COM, Aug. 25, 2008, http://www.ama-assn.org/amednews/2008/08/25/bisa0825.htm.

7. Nayla Kazzi, CENTER FOR AMERICAN PROGRESS, MORE AMERICANS ARE LOSING HEALTH INSURANCE EVERY DAY (MAY 4, 2009), http://www.americanprogress.org/issues/2009/05/pdf/healthinsurancelosses.pdf.

8. Hoffman & Podgurski, *supra* note 3, at 116–17.

9. *See infra* notes 99–106 and accompanying text.

10. *See* Jaan Sidorov, *It Ain't Necessarily So: The Electronic Health Record and the Unlikely Prospect of Reducing Health Care Costs*, 25 HEALTH AFF. 1079, 1080 (2006).

Because EHRs can consolidate information from all of a patient's doctors and require input of many more details than are traditionally noted in paper files, they can be voluminous. In addition, EHRs may be awkwardly organized, fragmented, incomplete, or otherwise difficult to understand when produced in printouts or Adobe Portable Document Format (PDF).[11] On the other hand, if EHRs are comprehensive and easily searchable, they could facilitate identification of relevant information and discovery of the truth.[12]

Finally, EHR systems will profoundly change the way health care providers operate. Health care professionals and their employees will need to learn to function in a world in which the computer is central to all aspects of patient care.

This Article will analyze the potential benefits and challenges that EHR systems will pose for the workplace. In order to address concerns arising from EHR system use, the Article argues for several legal and technical interventions. First, the Americans with Disabilities Act (ADA) should be amended to restrict pre-placement job testing and inquiries to matters that are job-related.[13] Second, the Health Insurance Portability and Accountability Act (HIPAA) and the HIPAA Privacy and Security Rules should be amended to cover employers.[14] Third, EHR technology must be improved to enhance EHR usability. All EHR products should enable providers to identify and disclose limited, discrete parts of patient records and should ensure that data is organized and displayed in ways that facilitate its use. Finally, a regulatory regime must be constructed to provide oversight that ensures the quality of EHR products.

The Article will proceed as follows. Part I will describe EHRs and EHR systems. Part II will analyze the relevant statutes: the ADA, the Genetic Information Non-Discrimination Act (GINA), the HIPAA Privacy and Security Rules, and relevant state laws. Part III will assess the impact of EHR systems on the workplace, and the concerns they raise for employees and employers. Part IV will formulate recommendations for legal and technical corrective measures that should be implemented as the country transitions to digitized medicine.

---

11. *See infra* notes 33–37 and accompanying text.

12. Sharona Hoffman & Andy Podgurski, *E-Health Hazards: Provider Liability and Electronic Health Records Systems*, 24 BERKELEY TECH. L.J. (forthcoming 2010) (describing EHR system attributes).

13. *See* 42 U.S.C. § 12112(d) (2006) (addressing medical inquiries and allowing employers to obtain unlimited medical information about individuals who have been given bona fide offers of employment but have not yet begun to work).

14. *See* 45 C.F.R. § 160.103 (2009) (defining "covered entity" as a health plan, health care clearing house, or a health care provider who transmits medical information in electronic form).

I. EHRS AND EHR SYSTEMS

An EHR can be defined as "[a] repository of electronically maintained information about an individual's lifetime health status and health care . . . ."[15] An EHR system is the "addition to an electronic health record of information management tools . . . ."[16] Comprehensive EHR systems go far beyond simply replacing paper files.[17] They display laboratory test results, patient allergies, lists of medications the patient is taking, medical and nursing diagnoses, patient demographics, and providers' notes.[18] EHR systems also electronically transmit test results from laboratories, radiology centers, and other testing facilities to clinicians quickly and efficiently.[19] Many systems allow clinicians to submit computerized medication orders and care instructions to pharmacies and other providers.[20]

In addition, EHR systems feature decision support capabilities, such as automatic alerts and reminders concerning patient allergies, appropriate diagnostic tests, potential drug interactions, and other matters.[21] EHR systems may further provide for secure messaging that allows doctors and patients to communicate electronically.[22] E-mail messages exchanged between patients and physicians could thus be captured by the EHR system and become part of the medical record.

Also of interest are personal health records (PHRs). A PHR is "[a]n electronic application through which individuals can access, manage and share their health information, and that of others for whom they are authorized, in a private, secure, and confidential environment."[23] Some PHRs are components

---

15. BIOMEDICAL INFORMATICS: COMPUTER APPLICATIONS IN HEALTH CARE AND BIOMEDICINE 937 (Edward H. Shortliffe & James J. Cimino eds., 3d ed. 2006) [hereinafter BIOMEDICAL INFORMATICS].

16. *Id.*

17. *See* INSTITUTE OF MEDICINE, COMMITTEE ON DATA STANDARDS FOR PATIENT SAFETY, KEY CAPABILITIES OF AN ELECTRONIC HEALTH RECORD SYSTEM 7 (2003), *available at* http://www.nap.edu/catalog.php?record_id=10781 (listing the core functions of an EHR system).

18. *Id.* at 7.

19. *Id.* at 7–8.

20. *Id.* at 8.

21. *Id.* at 8–9.

22. *See* Catherine Chen et al., *The Kaiser Permanente Electronic Health Record: Transforming and Streamlining Modalities of Care*, 28 HEALTH AFF. 323, 325 (2009) (describing the secure messaging system implemented by Kaiser Permanente Hawaii in September 2005).

23. Paul C. Tang et al., *Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption*, 13 J. AM. MED. INFORMATICS ASS'N 121, 122 (2006) (quoting MARKLE FOUNDATION, *CONNECTING FOR HEALTH: THE PERSONAL HEALTH WORKING GROUP FINAL REPORT* 14 (July 1, 2003), *available at* http://www.connectingforhealth.org/resources/final_phwg_report1.pdf). A PHR has also been defined as an "electronic record of . . . health information . . . on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." *See* Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act), 42 U.S.C.A. § 17921(11) (2010).

of EHR systems that are provided by hospitals, clinics, or physicians and allow patients to view appointment schedules, test results, and other information, and in some cases, to enter their own notations into the record. Other PHRs are stand-alone, independent products that allow patients to maintain and manage copies of their health records for their own use.[24]

Most relevant for purposes of this Article are PHRs that are constructed by employers. For example, Wal-Mart and other large employers, such as Intel and BP, with a total of 2.5 million employees, have formed a PHR system named Dossia.[25] Dossia's website explains that its "aggregated information includes health data from doctors offices, health plans, pharmacies and labs, as well as self-entered data," which is securely stored in the Dossia database and is available to individuals for life, even if they change employers.[26] Dossia represents that "[c]urrent or future employers, providers, and health insurers will never have access to this information without explicit consent from the user."[27] However, some commentators worry that health information stored on employer-provided PHRs may not be fully protected from the curious eyes of management officials.[28] It is also possible that employers seeking medical data will ask workers to sign release authorizations that allow them access to PHRs.

Ideally, EHR systems should be interoperable. "Interoperability" is the ability of "systems to exchange data and operate in a coordinated, seamless manner."[29] The federal government's goal is to achieve widespread interoperability by building a "nationwide health information technology infrastructure that permits the electronic exchange and use of health information."[30] Interoperability would allow authorized personnel to access patient records no matter where they are stored and by whom the patient was previously treated, including records created by clinicians in distant locations and other health care networks.[31] This capability might significantly improve health outcomes because doctors would always be able to refer to documentation concerning patients' medical histories, drug lists, allergies, and

24. John D. Halamka et al., *Early Experiences with Personal Health Records*, 15 J. AM. MED. INFORMATICS ASS'N. 1, 1 (2008).

25. *Patient Privacy Rights: Hearing Before the S. Subcomm. on Fed. Government Management, the Fed.Workforce, and the District of Columbia*, 110th Cong. at 5–6 (2007) (statement of Mark A. Rothstein, Director, Institute for Bioethics, Health Policy and Law, University of Louisville School of Medicine).

26. Dossia, *About Dossia*, http://www.dossia.org/about-dossia.

27. *Id.*

28. *See* Chris Dimick, *The Great PHRontier: Private Business Stakes a Claim in Personal Health Records*, 79 J. AHIMA 24, 28 (2008), *available at* http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_038462.hcsp?dDocName=bok1_038462 (discussing privacy concerns).

29. BIOMEDICAL INFORMATICS, *supra* note 15, at 952.

30. 42 U.S.C. § 300jj-12(b)(1) (2006).

31. Hoffman & Podgurski, *supra* note 3, at 112–13.

other critical matters.[32] Currently, doctors must often rely on the patient's own memory, and when patients arrive unconscious or in an uncommunicative state at emergency rooms, physicians often must treat them without access to potentially life-saving medical data. However, interoperability may also enable all authorized viewers, including employers, to see a patient's comprehensive medical record from birth until the present, without excluding psychiatric records, sexual history, and other sensitive information. In addition, because patient records could be accessed by many parties from across the country, interoperability will increase the possibility that details of a patient's medical history will be inappropriately disclosed to third parties.

According to many experts, contemporary EHR system technology has significant shortcomings, some of which affect the navigability and clarity of EHRs.[33] Computer systems often require users to enter elaborate data that create excessively voluminous records.[34] Cut and paste capabilities allow doctors to copy large portions of prior clinical notes into current updates for the sake of completeness, but this practice exacerbates the problem of information overload and can introduce errors if the notes are not carefully edited to eliminate outdated information.[35] In addition, EHRs can suffer from fragmentation. Information relevant to a particular medical problem may be found on numerous different screens and may be scattered throughout the record.[36] Furthermore, awkward information displays might make it difficult for users to scan EHRs for the particular facts they seek.[37] The excessive volume of EHRs, fragmentation, and other display problems might hinder production of discrete portions of EHRs to third parties. Thus, employers might receive unwarranted amounts of information in response to medical inquiries.

Furthermore, EHR printouts, although voluminous, may be incomplete and could be displayed or organized in a manner that makes them incomprehensible to untrained personnel. Computerized records often contain hyperlinks that provide important information. For example, a cholesterol test result may allow the viewer to press on a hyperlink that will reveal who ordered the test, why it was ordered, where the test was performed, and what

---

33. *See* Joan S. Ash et al., *Some Unintended Consequences of Information Technology in Health Care: The Nature of Patient Care Information System-related Errors*, 2 J. AMER. MED. INFORMATICS ASS'N 104, 107 (2004); *see also* Michael I. Harrison et al., *Unintended Consequences of Information Technological in Health Care- An Interactive Sociotechnical Analysis*, 14 J. AMER. MED. INFORMATICS ASS'N 542, 545 (2007).

34. *See* Joseph G. Cramer, *We Bought the Wrong EMR*, MED. ECON., Feb. 5, 2010, 28, 29.

35. Eugenia L. Siegler & Ronald Adelman, *Copy and Paste: A Remediable Hazard of Electronic Health Records*, 122 AM. J. MED. 495, 495–96 (2009).

36. *See* Ash et al., *supra* note 33, at 107; *see also* Harrison et al., *supra* note 33, at 545.

37. *See* Ross Koppel et al., *Role of Computerized Physician Order Entry Systems in Facilitating Medication Errors*, 293 J. AM. MED. ASS'N 1197, 1199–1201 (2005) (discussing information fragmentation and human-machine interface flaws).

the patient's prior cholesterol test results are. Printouts are unlikely to include the information in the hyperlinks. They are also unlikely to include evidence of decision support prompts or alerts that may have motivated a clinician to make particular medical decisions. In addition, fragmentation may make it difficult to follow the patient's medical history and progression. For example, EHR data may be organized simply by reverse chronological order. Thus, the patient's most recent cholesterol test results may be printed on page 200 of the EHR hard copy, and the prior cholesterol number may be found on page 100. EHR printouts are not produced with tabs, cover sheets, and other mechanisms designed to facilitate the task of finding necessary information. Reviewing EHR printouts can thus be burdensome, frustrating, and at times, fruitless.

II. THE RELEVANT LAWS: THE ADA, GINA, HIPAA, AND STATE STATUTES

It is not uncommon for employers to obtain applicants' and employees' medical records. According to one source, every year more than ten million workers sign authorizations for release of medical information before the commencement of their employment.[38] Employers may process medical information for purposes of determining fitness for duty, reasonable accommodations, workers' compensation, FMLA requests,[39] and insurance claims.[40] It is thus appropriate to ask: under what circumstances is it lawful for employers to obtain medical information, and what are they permitted to do with the data?

This section will review the major federal laws that govern employers' acquisition and use of health information insofar as that information could be stored in EHRs. It will address the ADA, GINA, the HIPAA Privacy and Security Rules, and relevant state laws.

A. The Americans with Disabilities Act

Employers frequently obtain medical information relating to employees through medical examinations or inquiries to determine whether an employee is qualified for a particular job and for purposes of providing reasonable accommodations to individuals with disabilities. Title I of the ADA prohibits employment discrimination with respect to job application procedures, hiring, promotion, termination, compensation, training, and all other conditions and benefits of employment.[41] Congress recently revised the ADA by enacting the

38. *See* Mark A. Rothstein & Meghan K. Talbott, *Compelled Authorizations for Disclosure of Health Records: Magnitude and Implications*, 7 AM. J. BIOETHICS 38, 40 tbl. 1 (2007).

39. The FMLA requires only a certification from a health care provider with facts relevant to the condition in question. 29 U.S.C. § 2613(b)(3) (2006). Thus, employers may not receive actual portions of the EHR in conjunction with an FMLA request.

40. *See supra* notes 4–6 and accompanying text.

41. *See* 42 U.S.C. § 12112(b)(1) (2006). Title I of the ADA applies to employers with

ADA Amendments Act of 2008,[42] which significantly broadened the category of individuals who are deemed to have disabilities under the statute.[43] The Rehabilitation Act of 1973 provides similar protection to federal employees,[44] though this discussion will focus on the ADA. Despite this anti-discrimination mandate, the more information an employer receives about an employee and the more predictive it is of future health problems, the more workers may be concerned that employers will base employment decisions on the medical details they learn. EHRs will likely provide employers with unprecedented amounts of data.

1. Pre-placement Examinations

The ADA governs employer-conducted medical examinations and inquiries.[45] Prior to extending a job offer to an applicant, an employer may not ask a candidate about any medical conditions or physical or mental limitations other than inquiring as to whether the individual can perform specific job-related tasks.[46] Existing employees can be subjected only to medical tests and inquiries that are "job-related and consistent with business necessity."[47] However, employers have a window of opportunity to obtain medical information that is much broader in scope. After extending an offer of employment to a candidate but before the commencement of employment, an employer is permitted to conduct unrestricted medical examinations or inquiries so long as all entering employees are subjected to the same queries or testing.[48] Post-offer, pre-placement medical examinations do not need to be job related or justified by business necessity.[49] Nothing in the statute would stop an employer from asking individuals to sign authorizations that would release their entire EHRs to the employer.

The ADA requires that all medical information obtained about applicants and employees be kept confidential.[50] Medical information must be stored separately and cannot be combined with general personnel files.[51] However, the ADA does not impose administrative penalties on employers who violate

---

fifteen or more employees who are engaged in an industry affecting commerce, employment agencies, labor organizations, and joint labor-management committees. *See* §§ 12111(2), (5)(A).

42. Pub. L. No. 110-325, 122 Stat. 3553.

43. "Disability" is defined in part as a "physical or mental impairment that substantially limits one or more major life activities of . . . [an] individual." 42 U.S.C. § 12102(1)(A). For explanation of 2008 amendments see *infra* note 91 and accompanying text.

44. *See* 29 U.S.C. §§ 701–796l (2006).

45. *See* 42 U.S.C. § 12112(d).

46. *See id.* § 12112(d)(2).

47. *Id.* § 12112(d)(4)(A).

48. *See id.* § 12112(d)(3). *But see* GINA, *infra* Part II.B (prohibiting employers from seeking genetic information).

49. 29 C.F.R. § 1630.14(b)(3) (2009).

50. 42 U.S.C. § 12112(d)(3)(B), (4)(C) (2006).

51. *Id.*

the confidentiality mandate. Consequently, employers would likely be held accountable only if an individual is harmed by an improper disclosure and that individual initiates litigation.

2. Reasonable Accommodation Requests

The ADA requires employers to provide reasonable accommodations to applicants and employees who have disabilities but are otherwise qualified to perform the job in question.[52] Employers may decline to provide reasonable accommodations that would impose an undue hardship on them.[53]

Medical information that is obtained pursuant to employment testing or inquiries may be disclosed to supervisors for purposes of providing reasonable accommodations.[54] In addition, upon receiving a request for accommodation, the employer may ask the employee to provide medical information or to sign a release in order to confirm the need for an accommodation and to identify a modification that would meet the individual's needs.[55]

B. The Genetic Information Nondiscrimination Act

GINA, enacted in 2008, places further constraints upon employers' medical inquiries.[56] The statute amends Title VII of the Civil Rights Act of 1964 and establishes that it is unlawful for employers to discharge, refuse to hire, or make employment decisions relating to compensation or the terms and privileges of employment based on an employee's genetic information.[57] Employers also may not use genetic information to classify employees in ways that would decrease their employment opportunities or adversely affect their

52. *See id.* § 12112(b)(5)(A). The regulations provide that a qualified individual with a disability is someone who "satisfies the requisite skill, experience, education and other job-related requirements of the employment position . . . and who, with or without reasonable accommodation, can perform the essential functions of such position." 29 C.F.R. § 1630.2(m). Reasonable accommodations can include making existing facilities accessible to the individual, providing a part-time or modified work schedule, job reassignment, purchasing or modifying equipment or devices, revising examinations, training materials, or policies, and providing qualified readers or interpreters. *See id.* § 1630.2(o).

53. *See id.* § 12112(b)(5)(A). The following factors should be considered in the process of determining whether providing a particular accommodation would impose an undue hardship on an employer: the nature and net cost of the accommodation, the employer's overall financial resources, the resources of the facility at which the individual would work, the type of operation run by the employer, and the accommodation's impact on the operation of the facility in question. 29 C.F.R. § 1630.2(p).

54. 42 U.S.C. § 12112(d)(3)(B)(i).

55. *See* 29 C.F.R. § 1630.2(o)(3) (2009); *see also* Beck v. Univ. of Wis. Bd. of Regents, 75 F.3d 1130, 1136 (7th Cir. 1996) (ruling against an employee who failed to sign a release so the employer could obtain information from her doctor concerning her accommodation needs).

56. 42 U.S.C.A. § 2000ff-1 (2010).

57. *Id.* § 2000ff-1(a).

status.[58] Furthermore, self-insured employers acting as group health insurers are forbidden by law to use genetic information to discriminate against an individual by denying coverage, conditioning coverage or policy issuance, or pricing a policy on the basis of genetic information.[59]

Of particular significance in the EHR context is that GINA prohibits employers from requesting, requiring, or purchasing genetic information about employees or their family members.[60] GINA also bars employers who serve as group health insurers from requesting or requiring genetic information about individuals for underwriting or enrollment purposes.[61]

These restrictions suggest that employers should never be able to access genetic information contained in applicants' or employees' EHRs. However, GINA does not prohibit employers from asking applicants and employees to sign authorizations for release of their medical records for various lawful reasons, such as fitness for duty determinations.[62] Consequently, it is possible that employers will receive genetic information when they obtain electronic files in response to such authorizations.[63] Given the complexity of EHRs,[64] it is unlikely that providers would have the time, inclination, or even ability to carefully redact genetic information from patient records.

Moreover, as scientists discover that genetic factors are implicated in a growing number of health problems, it is increasingly difficult to define what "genetic" means.[65] GINA, for example, includes "the manifestation of a disease or disorder in [one's] family members" in the definition of "genetic information."[66] Thus, even a notation that the patient's mother had a heart attack or breast cancer could be considered genetic data because the parent's illness may be predictive of the patient's future health vulnerabilities. Such information is not likely, however, to be identified by providers as genetic and deliberately eliminated from records they disclose to employers. In short, GINA may not significantly restrict employers' access to EHR data.

C. The HIPAA Privacy and Security Rules

Providers' disclosure of medical information to third parties, including employers, is governed by HIPAA regulations. The HIPAA Privacy Rule and

58. *Id.*

59. *See id.* §§ 300gg-1(a)(1)(F), 300gg-1(b)(3). Health insurers offering group plans are also prohibited from discriminating against individuals based on disability. *Id.* § 300gg-1(a)(H).

60. *Id.* § 2000ff-1(b).

61. 42 U.S.C. § 300gg-1(c)-(d) (2006).

62. *See id.* § 2000ff-1(b).

63. *See* Rothstein, *supra* note 4, at 177 (arguing that employers will continue to obtain genetic information because there is no way to easily redact it from EHRs).

64. *See supra* notes 33- 37 and accompanying text.

65. *See* Rothstein, *supra* note 4, at 177 ("it is impossible to define 'genetic' when scientists have identified that genes play a role in virtually every human health problem").

66. 42 U.S.C.A. § 2000ff(4)(A)(iii) (2010).

the HIPAA Security Rule were issued pursuant to HIPAA legislative authority.[67] The Rules apply to protected health information (PHI), which is "individually identifiable health information" that is electronically or otherwise transmitted or maintained.[68] The Rules cover a limited range of health-related entities, namely, health plans, health care clearinghouses, and health care providers who transmit health information electronically for particular purposes, generally claims or benefits activities.[69] Congress amended the HIPAA Privacy and Security Rules in 2009 to extend to these entities' business associates as well.[70] However, employers are not per se covered entities and are bound by the Rules' mandates only to the extent that they operate as health insurers.

The Privacy Rule's "uses and disclosures" provision prohibits covered entities from utilizing and disseminating PHI without the patient's consent except in specific circumstances that generally relate to medical treatment, payment, health care operations, public health needs, or other obligations established by law.[71] Employers who are self-insured can receive medical information from providers for payment purposes without their employees' authorization. Such employers are considered "hybrid" entities whose business activities include both covered (insurance) and non-covered (employment) functions.[72]

The Privacy Rule requires covered entities that use or disclose PHI or request it from other entities to "make reasonable efforts to limit" the released information "to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."[73] EHRs, however, may make it difficult for clinicians responding to an employer's request for information to isolate the minimum necessary to satisfy the employer's needs. EHRs may integrate all of a patients' data from different doctors concerning different medical conditions, though they may not be organized in a manner conducive to producing small portions of the record based on subject matter.[74]

The HIPAA Security Rule is designed to ensure the security of electronically stored health information. The Rule imposes four general requirements upon covered entities. They must (1) ensure the "confidentiality, integrity, and availability" of PHI; (2) safeguard against reasonably anticipated security threats to the data; (3) protect against reasonably anticipated prohibited uses and disclosures of the data; and (4) ensure that their workforces

---

67. *Id.* §§ 1320d-1–1320d-3 (requiring the HHS Secretary to establish standards and implementation specifications for electronic health information).

68. 45 C.F.R. § 160.103 (2009).

69. *Id.*

70. 42 U.S.C.A. § 17931.

71. 45 C.F.R. §§ 164.502, 164.512.

72. *Id.* §§ 164.103, 164.105.

73. *Id.* §§ 164.502(b)(1).

74. *See supra* notes 33–37 and accompanying text.

comply with the Rule.[75] To this end, the HIPAA Security Rule establishes administrative, physical, and technical safeguards with which covered entities must comply.[76] Because employers are not covered entities, they are not required to implement the security measures specified in the Rule and may not adequately protect health information that they possess. Only employers serving as insurers would be bound by the Rule insofar as they handle claims-related PHI.[77]

D. Relevant State Laws

State law further governs disclosure of EHRs to employers. State statutes parallel or supplement federal mandates that prohibit discrimination and protect employees' privacy. Workers' compensation statutes, on the other hand, establish requirements for medical disclosures in particular circumstances.

All fifty states have their own disability rights statutes.[78] These laws vary in scope and coverage, and many do not discuss or limit medical inquiries.[79]

---

75. 45 C.F.R. § 164.306(a) (2009).

76. *Id.* §§ 164.308(a), 164.310, 164.312. Administrative safeguards focus on the following areas: security management processes, workforce security, information access management, security awareness and training, security incident procedures, and contingency plans. Implementation specifications require risk assessment, the creation of a sanctions policy for non-compliant employees, workforce clearance procedures, log-in monitoring, password management, and many other measures. The physical safeguards section of the Security Rule addresses facility access controls, workstation use, workstation security, and device and media controls. Implementation specifications instruct covered entities to develop a number of plans and procedures including those related to facility security, access control and validation, and data backup and storage. The Rule's technical safeguards section mandates the establishment of procedures to control PHI access, to audit activity in information systems that process PHI, to protect PHI from inappropriate modification or eradication, to obtain authentication from PHI users, and to protect PHI. The implementation specifications address matters such as encryption, decryption, and authentication mechanisms. For a critique of the HIPAA Security Rule see Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331, 338–44 (2007).

77. *See* 45 C.F.R. §§ 164.103, 164.105; Brian K. Powell & Richard A. Bales, *HIPAA as a Political Football and Its Impact on Informal Discovery in Employment Law Litigation*, 111 PENN. ST. L. REV. 137, 149–52 (2006).

78. Ruth Colker & Adam Milani, *The Post-*Garrett *World: Insufficient State Protection Against Disability Discrimination*, 53 ALA. L. REV. 1075, 1075 (2002); Sharona Hoffman, *Preparing for Disaster: Protecting the Most Vulnerable in Emergencies*, 42 U.C. DAVIS L. REV. 1491, 1528 (2009).

79. ABA Comm. on State Labor Law Developments, *State Labor Law Developments*, 9 LAB. LAW. 221, 247 (1993) ("many state laws do not provide the clear guidance that the ADA does on the issue of medical exams and inquiries"). *But see* ARIZ. REV. STAT. ANN. § 41-1466 (2009); CAL. GOV'T CODE § 12940 (West 2004); IND. CODE § 22-9-5-20 (2009); ME. REV. STAT. ANN. tit. 5, § 4572 (2009); MINN. STAT. ANN. § 363A.20 Sub.8. (West 2009); NEB. REV. STAT. Ann. § 48-1107.02 (2009); OR. REV. STAT. §§ 659A.133, 659A.136 (2007); S.C. CODE ANN. § 1-

The laws generally prohibit disability-based employment discrimination and establish reasonable accommodation requirements. Furthermore, forty-four states and Washington, D.C., have laws that address the use of genetic information by health insurers,[80] and thirty-four states and Washington, D.C., prohibit genetic discrimination by employers,[81] though these laws, like the disability statutes, vary in their substantive contents.

In addition, numerous state laws provide patients with privacy rights.[82] For example, California residents have a right to privacy under the state constitution,[83] and are protected against disclosure of medical records without their consent by the California Confidential Medical Information Act.[84]

All states have workers' compensation laws that require employers to report workplace injuries and compensate employees for them.[85] In order to determine the appropriate amount of compensation, workers' compensation carriers ask injured employees to produce medical documentation or sign a medical records release form.[86] If the employer is self-insured for workers' compensation purposes, medical documentation about injured workers is disclosed directly to the employer.[87]

III. THE IMPACT OF EHRS ON THE WORKPLACE

The advent of EHR systems will have far-reaching effects on the workplace. It may focus renewed attention on discrimination and privacy issues. EHRs will have cost implications and will require all those handling medical information to adjust to the advantages and disadvantages of the computerized format. This section will explore the technology's impact on both employees and employers.

A. Increased Employee Concerns about Discrimination and Privacy

The storage of medical records in an electronic format may cause employers to obtain unprecedented amounts of medical information in

---

13-85 (2008).

80. National Conference of State Legislatures, Genetic and Health Insurance State Anti-Discrimination Laws (March 2008), http://www.ncsl.org/IssuesResearch/Health/GeneticNondiscriminationinHealthInsuranceLaws/tabid/14374/Default.aspx.

81. National Conference of State Legislatures, Genetic Employment Laws, (Jan. 2008), http://www.ncsl.org/IssuesResearch/Health/GeneticEmploymentLaws/tabid/14280/Default.asp.

82. Hoffman & Podgurski, *supra* note 12.

83. CAL. CONST. art. I, § 1.

84. CAL. CIV. CODE § 56.10 (West 2010).

85. James G. Hodge, Jr., *The Intersection of Federal Health Information Privacy and State Administrative Law: The Protection of Individual Health Data and Workers' Compensation*, 51 ADMIN. L. REV. 117, 119 (1999).

86. *Id.* at 125.

87. *Id.*

response to legitimate requests for health records. Existing laws, including the ADA, GINA, HIPAA, and their state counterparts, provide important assurances to applicants and employees but are insufficient to guarantee that they will suffer no ill consequences as a result of EHR disclosure to employers. Employees may be especially concerned in times of recession, knowing that financial pressures make workers with health problems particularly unattractive to employers. Employers or their hired experts may develop complex scoring algorithms based on EHRs to determine which individuals are likely to be high-risk and high-cost workers. In addition, in times of financial difficulty, limited resources may be available to implement technology and policies that will secure EHR confidentiality.

Despite the anti-discrimination mandates of the ADA and equivalent state laws, employees continue to worry about being subjected to discrimination because of their disabilities. The Equal Employment Opportunity Commission (EEOC) reports that in Fiscal Year 2008 it received 19,453 charges of discrimination involving disability claims.[88] The existence of EHRs and the wealth of information they may offer employers will justifiably intensify employees' concern about discrimination.

Plaintiffs often find it difficult to prove discrimination in employment cases. Consequently, employers may be willing to risk litigation in order to avoid hiring individuals with disabilities who may require accommodation or frequent medical treatment that will raise insurance costs. Surveys of ADA litigation that was resolved by courts (rather than through settlement) revealed that plaintiffs prevailed in as few as three percent of cases.[89] In the past, these low plaintiff win rates were attributed, at least in part, to the ADA's narrow definition of the term "disability."[90] The 2008 ADA Amendments Act significantly broadened the category of individuals who are deemed to have disabilities, and most serious medical conditions will be covered disabilities

88. U.S. Equal Employment Opportunity Comm'n, Americans with Disabilities Act of 1990 (ADA) Charges FY 1997—FY 2009, http://www.eeoc.gov/eeoc/statistics/enforcement/ada-charges.cfm.

89. *See* Amy L. Allbright, *2004 Employment Decisions Under the ADA Title I—Survey Update*, 29 MENTAL & PHYSICAL DISABILITY L. REP. 513, 513 (2005). The article discusses surveys of federal court cases found through Westlaw searches and gathered from "various media outlets." The surveys considered an employer to have won the case if the plaintiff's complaint was dismissed or the employer prevailed on the merits, and an employee to have won if she prevailed on the merits. Opinions resolving preliminary matters, such as those denying summary judgment to employers, were considered to render neither party a winner, because they led to no final resolution, and thus, were not included in the surveys' calculations. *Id.*

90. *See* Michael H. Fox & Robert A. Mead, *The Relationship of Disability to Employment Protection Under Title I of the ADA in the United States Circuit Courts of Appeal*, 13 KAN. J.L. & PUB. POL'Y 485, 489 (2004) (commenting that "only a surprisingly narrow band of individuals with disabilities are protected by [the ADA]"); *see also* Sharona Hoffman, *Corrective Justice and Title I of the ADA*, 52 AM. U. L. REV. 1213, 1224 (2003) (discussing the courts' restrictive interpretation of the term "disability").

under the law.[91] However, plaintiffs will still find it challenging to prove that adverse employment decisions are linked to their disability status and were motivated by employers' intent to discriminate.[92] Proving discrimination essentially requires a plaintiff to enter the mind of the employer and establish what the employer was thinking at the time it made its decision. Without "smoking gun" verbal or written comments or other obvious evidence concerning discriminatory conduct, plaintiffs are at a great disadvantage.

Employers with access to EHRs containing a wealth of medical information may be sorely tempted to exclude certain individuals from the workforce because of concerns about the employees' future productivity, absenteeism, or medical costs. To disguise unlawful conduct, employers may not act immediately to withdraw a job offer or terminate an employee, but rather, decide not to promote an individual with a disability or to select her for a layoff at a later time. It may be difficult, if not impossible, for plaintiffs to associate such decisions with earlier disclosures of medical information for purposes of proving ADA violations.[93]

Employees may also be concerned about privacy risks involving electronic health information possessed by employers. If data security is breached, employees' private information can be distributed on the Internet to countless people worldwide.[94] Disclosure of psychiatric history, HIV status, or other sensitive information can lead to many personal and professional harms.[95] In addition, it is estimated that between 250,000 and 500,000 patients suffer medical identity theft each year.[96] In medical identity theft cases, personal information is stolen for purposes of Medicare fraud and other

---

91. *See* 42 U.S.C.A. § 12102 (2010). The ADA Amendments define "major life activities" as including, but not limited to, "caring for oneself, performing manual tasks, seeing, hearing, eating, sleeping, walking, standing, lifting, bending, speaking, breathing, learning, reading, concentrating, thinking, communicating, and working." *Id.* § 12102(2)(A). Further, major life activities include operation of major bodily functions such as, "functions of the immune system, normal cell growth, digestive, bowl, bladder, neurological, brain, respiratory, circulatory, endocrine, and reproductive functions." *Id.* § 12102(2)(B) "The definition of disability in this chapter shall be construed in favor of broad coverage of individuals." *Id.*; Pub. L. No. 110-325, 122 Stat. 3553 (2008) ("the question of whether an individual's impairment is a disability under the ADA should not demand extensive analysis").

92. Sheridan v. E.I. DuPont de Nemours & Co., 100 F.3d 1061, 1071 (3rd Cir. 1996) (en banc) ("Cases charging discrimination are uniquely difficult to prove and often depend upon circumstantial evidence."); Thornbrough v. Columbus & Greenville R.R. Co., 760 F2d 633, 638 (5th Cir. 1985) ("Unless the employer is a latter-day George Washington, employment discrimination is as difficult to prove as who chopped down the cherry tree.").

93. If multiple employees are subjected to adverse decisions because of disabilities, it may eventually be possible to discern a pattern of misconduct on the part of the employer.

94. Hoffman & Podgurski, *supra* note 76, at 334–35.

95. *See id.*

96. Judith Graham, *Medical Identity Theft Spreads: Purloined Data Often the Crime of Insiders*, CHI. TRIB., August 22, 2008, at 10

financial gain.[97] Criminals might be particularly tempted to target workplace computer systems if they suspect that these are less secure than those found in hospitals or physicians' offices.

While the ADA mandates that medical information be stored separately from general personnel files,[98] the statute, which was passed in 1990, assumed that records would be in paper format and could be locked in separate filing cabinets. It does not address the need for encryption, password authorization, and other security safeguards for electronic records that will be stored by employers. While the HIPAA Security Rule imposes certain security requirements on covered entities, it binds employers only to the extent that they act as insurers.[99] Thus, EHRs and PHRs that are handled by employers may be vulnerable to hacking, laptop theft, and other forms of intentional or accidental unauthorized disclosure.[100]

B. Employer Concerns

The use of EHRs will impact not only employees, but also employers. Technologically sophisticated employers may welcome the introduction of computerized records, and EHRs may ultimately reduce costs. However, some employers will find that they are more difficult to read or understand for purposes of determining health-related worker qualifications. In addition, EHR use will make employers vulnerable to privacy breaches and could affect employers' insurance costs. It will also change how discovery is conducted when medical records are at issue and will profoundly affect the work habits of health care providers.

1. Employment Testing

Employers themselves may be frustrated by the need to handle EHRs and may find them far more cumbersome and abstruse than paper records. EHR printouts or PDFs may create a confusing picture of the medical chart and be difficult for lay employers to interpret.[101] They may be both voluminous and incomplete and contain data that is organized poorly, displayed awkwardly, or fragmented throughout the document—all of which would thwart the employer's ability to determine whether an applicant or employee has a condition that disqualifies her from performing essential job tasks.[102]

---

97. *Id.*; Daniel Kim et al., *A Physician's Role Following a Breach of Electronic Health Information*, 21 J. CLIN. ETHICS (forthcoming 2010) (discussing harms associated with medical identity theft).

98. 42 U.S.C. § 12112(d)(3)(B) (2006).

99. *See supra* notes 72, 75–77 and accompanying text.

100. *See* Hoffman & Podgurski, *supra* note 12 (discussing privacy breaches).

101. Anne Armstrong-Coben, *The Computer Will See You Now*, N.Y. TIMES, Mar. 6, 2009, at A27 ("In the past, I could pick up a chart and flip through it easily . . . . Now . . . important points often get lost.").

102. *See supra* notes 34–37 and accompanying text.

The computerization of medical records could have varying consequences in the area of employment testing. Some employers may be comfortable reading EHRs and find them more informative than traditional paper records that contain illegible hand-writing or summary dictation. Some may choose to retain experts who offer record screening services, interpret EHRs, and provide summaries or scores to the employer. Other employers may misinterpret bewildering EHRs, erroneously conclude that individuals have serious medical problems, and wrongly deprive workers of employment opportunities. Still others may opt to forego using EHRs and subject employees to actual medical testing. If employers do not request access to EHR records, workers will enjoy greater privacy protection, but some may resent undergoing physical exams or distrust company doctors who are tasked with conducting them.

2. Other Impacts

EHR systems may affect employers in several other ways as well. While employees will likely be anxious about the confidentiality of their electronic health records, employers should be equally concerned about their ability to maintain the security of digitized information. Health data stored by employers may be vulnerable to hacking, theft, or inappropriate disclosure by imprudent co-workers. If personal health information is inappropriately leaked or divulged, employers can be sued under state common law or statutory causes of action relating to privacy.[103]

EHR systems will also impact medical costs, which will in turn influence employer expenses. In the short term, the purchase, implementation, and maintenance of EHR systems is expensive, costing tens of thousands of dollars per physician,[104] though, under the stimulus legislation, government stipends should cover some of these expenses in the near future.[105] Furthermore,

---

103. *See* Hoffman & Podgurski, *supra* note 12.

104. *See* Thomas Goetz, *Physician, Upgrade Thyself*, N.Y. TIMES, May 30, 2007, at A21 (estimating that the purchase of an EHR system costs $33,000 per doctor, with an added $1,500 a month per doctor for maintenance); *see also* Richard J. Baron et. al., *Electronic Health Records: Just Around the Corner? Or Over the Cliff?*, 143 ANNALS OF INTERNAL MED. 222, 222–24 (2005) (reporting that an EHR system cost a four-person medical practice $140,000, including hardware, software, training, and one year of support, and its estimated annual maintenance cost, including support services, was $40,000); *see also* THE HOSPITAL & HEALTHSYSTEM ASS'N OF PA., IMPROVING PATIENT CARE: PENNSYLVANIA HOSPITALS' USE OF INFORMATION TECHNOLOGY 2 (2007), http://www.haponline.org/downloads/Improving_Patient_Care_PA_Hospitals_Use_of_IT_HAP_082007.pdf (reporting that Pennsylvania's median capital spending per bed for HIT in 2006 was $6,912, while the median HIT operating cost in the state was $14,528).

105. *See* Blumenthal, *supra* note 2, at 1477–78 (reporting that President Obama's stimulus plan will offer payments of up to $44,000 per physician over 5 years for meaningful use of certified EHR systems); *see also* Taylor Burke, *The Health Information Technology Provisions in the American Recovery and Reinvestment Act of 2009: Implications for Public Health Policy and Practice*, 125 PUB. HEALTH REP. 141, 143–45 (2010), *available at* http://www.publichealthreports.org/userfiles/125_1/141-145.pdf (discussing Medicare and Medicaid HIT adoption incentives and their implications).

flawed technology or use by untrained and unskilled clinicians can lead to costly medical errors.[106] For example, software glitches in the VA's EHR system exposed veterans to excessive and potentially life-threatening dosages of the blood-thinner Heparin.[107] In addition, EHR systems are believed by many to offer providers improved ways to calculate and record charges and thus to maximize income.[108] These costs may well be passed on to patients and employers who offer insurance coverage. Employers that are self-insured pay medical claims directly and will have higher out-of-pocket expenditures with larger or more frequent claims. Employers that contract with third-party insurers may be subject to higher premiums if the cost of covering their employee groups increases.

By contrast, advocates argue that in the long term, if the country achieves a national health information network, cost savings associated with greater efficiency could reach a dramatic $77 billion per year.[109] Employers that offer health insurance would undoubtedly benefit from such eventual reductions in health care expenses, though there is little contemporary evidence of immediate cost savings.[110]

Employers involved in litigation relating to worker injuries or disabilities will in the future encounter EHRs rather than traditional medical files in discovery. Like employers seeking to determine fitness for duty, litigants will need to grapple with the complexities of electronic records. They may find that EHR printouts or PDFs are disjointed, confusing, incomplete and otherwise flawed in ways that impede discovery and distort medical records.[111]

---

106. *See* Hoffman & Podgurski, *supra* note 12.

107. Hope Yen, Veterans Exposed to Incorrect Drug Doses, BlueCross BlueShield Association (Jan. 13, 2009), http://www.bcbs.com/news/national/veterans-exposed-to-incorrect-drug-doses.html.

108. Hoffman & Podgurski, *supra* note 3, at 116-17 (citations omitted). *See also* RevenueXL, Does an Electronic Medical Record / Electronic Health Record Software System Increase Revenues? (Feb. 3, 2009), http://www.revenuexl.com/does-emr-ehr-increase-revenues (detailing how EHR software improves charge capture and maximizes billing).

109. Jan Walker et. al., *The Value of Health Care Information Exchange and Interoperability*, HEALTH AFF. W5-10, W5-16 (2005).

110. *See* Emma Schwartz, *Can Cleveland Clinic Be a Model for Digital Medicine?*, HUFFINGTON POST, Dec. 2, 2009, http://www.huffingtonpost.com/2009/12/02/can-cleveland-clinic-be-a_n_376842.html (explaining that for the Cleveland Clinic, "after nearly a decade and a $100 million investment, cost savings have not materialized and hospital officials are not certain when they will"); Caroline Lubick Goldzweig et al., *Costs and Benefits of Health Information Technology: New Trends from Literature*, 28 HEALTH AFF. w282, w292 (2009) (discussing the dearth of meaningful cost-benefit data concerning EHR system implementation).

111. *See* Kevin F. Brady et al., *E-Discovery in Healthcare & Pharmaceutical Litigation: What's Ahead for ESI, PHI & EHR?*, 9 SEDONA CONF. J. 167, 174-75 (2008) (identifying issues with computer stored records); *see also* Cecily Walters, *Attorney Survey Reveals Concerns About Litigation Costs*, TRIAL, Feb. 2009, at 64 (reporting that in responding to a survey of fellows of the American College of Trial Lawyers, "more than 87 percent said that e-discovery increases litigation costs, and almost 77 percent indicated that courts 'do not understand the difficulties in

At the same time, with optimal technology, EHRs could facilitate discovery. If all medical interventions are faithfully recorded in EHRs, computerized records could be more comprehensive than paper files built upon dictation of physicians' summary notes or often illegible hand-written notations. Similarly, if EHRs are interoperable and different physicians' records can be combined into one electronic patient file, discovery could yield a patient's entire medical history from birth until the present time through one document request from one source. Thus, for example, employers might be able to determine easily whether a patient had a pre-existing condition that affected a claimed workplace injury. EHR systems could also allow for electronic searches of medical files so that relevant details are found quickly and with little effort.[112]

Finally, employers that are health care providers will experience significant changes with EHR system implementation. EHR systems can improve the ability of physicians to meet patient expectations and enhance their job satisfaction.[113] They can allow physicians to better communicate with patients, more easily research patient information, easily find relevant medical literature, and enjoy other benefits.[114] However, transitioning to an EHR system can pose considerable challenges to clinicians who have become accustomed to operating in a world of paper records. Difficulties might include the following: (1) all users must adjust to entering all data that is required by the system in the system's preferred format and must forego their own shorthand and methods of keeping patient charts; (2) relevant information from paper charts must be moved to the electronic system, a process that can be time-consuming and complicated; (3) all staff members must learn to be adept at operating the system, and their training takes time away from patient care; and (4) patients may resent providers looking at computers at the bedside or in the examination room rather than at them.[115] Furthermore, many clinicians may find that EHR systems increase the time they must spend on documentation thereby, decreasing the time they have available for patient interaction.[116] This is so because typing takes physicians longer than dictating

---

providing e-discovery.'"); *see also supra* notes 34–38 and accompanying text (explaining issues specifically related to EHR technology).

112. *See* FED. R. CIV. P. 26 advisory committee's note to 26(b)(2) (stating that "[e]lectronic storage systems often make it easier to locate and retrieve information").

113. Baron et al., *supra* note 104, at 225. *See* Hoffman & Podgurski, *supra* note 3, at 112–119 (discussing the benefits of EHRs).

114. Baron et al., *supra* note 104, at 225–26.

115. *See id.* at 223–24; Ken Terry, *IT Implementation: Why EHRs Falter*, MED. ECON., Apr. 7, 2006, http://www.memag.com/memag/content/printContentPopup.jsp?id=316528; *see also* Ceci Connolly, *Cedars-Sinai Doctors Cling to Pen and Paper*, WASH. POST., Mar. 21, 2005, at A01.

116. *See* Yong Y. Han et al., *Unexpected Increased Mortality After Implementation of a Commercially Sold Computerized Physician Order Entry System*, 116 PEDIATRICS 1506, 1510 (2005) (asserting that computerized provider-order entry systems require more time for orders than do written forms); Jon Patrick, A Critical Essay on the Deployment of an ED Clinical Information System: Systemic Failure or Bad Luck?, http://www.it.usyd.edu.au

notes[117] and EHR systems demand numerous details that providers may not otherwise record.[118]

In short, EHR systems will have a profound impact on the American workplace. They will affect pre-placement medical inquiries, employers' storage of health data, employers' business costs, discovery in cases involving employee health, and the work habits of health care providers.

IV. RECOMMENDATIONS

The advent of EHR systems requires several modifications to the ADA and parallel state laws that address employment discrimination. The likelihood that EHRs will be disclosed to many employers in response to employees' authorizations to release medical information necessitates modification of the HIPAA Privacy and Security Rules and state privacy laws. In addition, those designing EHR systems must continue to strive to improve them so that EHRs can be summarized, excerpted, and easily navigated and understood by viewers. Finally, the federal government must establish a regulatory structure to oversee the quality and safety of EHR products.

A. Amending the Medical Testing Provisions of the ADA and State Laws

As noted above, the ADA allows employers to request unlimited medical data (other than genetic information) after extending a bona fide job offer to a candidate but before the commencement of employment.[119] The statute's failure to restrict such medical inquiries to those that are job-related was always puzzling. However, it is all the more troubling in light of EHRs, which may allow employers who obtain release authorizations to view individuals' comprehensive medical records including all details from birth until the present time.

Consequently, the time is ripe for Congress to eliminate the discrepancy between the ADA provision addressing pre-placement medical examinations and the provision addressing testing of incumbent employees, which must be

---

/~hitru/essays The%20Story%20of%20the%20Deployment%20of%20an%20ED%20Clinical%20Information%20System6.0.pdf (discussing the time required for data entry into the Firstnet EHR system) (last visited Feb. 14, 2010); Lise Poissant et al., *The Impact of Electronic Health Records on Time Efficiency of Physicians and Nurses: A Systematic Review*, 12 J. AM. MED. INFORMATICS ASS'N 505, 508 (2005) (finding that using bedside or examination room computers increased physician documentation time by 17.5%, and using centrally located desktops for electronic medication orders rather than prescription pads increased physician time by 98.1 percent to 328.6 percent).

117. Baron et al., *supra* note 104, at 223–24.

118. *See* Armstrong-Coben, *supra* note 101, at A27 (asserting that the EHR system requires her "to bring up questions in the order they appear [and] to ask the parents of a laughing 2-year-old if she is 'in pain'").

119. 42 U.S.C. § 12112(d)(3) (2006).

job-related.[120] As I have argued in previous work, pre-placement medical inquiries, like their post-placement counterparts, should be restricted in scope. The ADA should allow employers to obtain health information and administer medical tests only to the extent that the data they seek is job-related and justified by business necessity.[121] Rather than obtaining general authorizations for release of all medical records, employers should be permitted to pose only narrowly tailored queries that are designed to determine fitness for duty.

It must be recognized that extracting relevant information from EHRs will be a work-intensive task for health care providers that will require judgment and time. For example, if an employer asks for any information that is relevant to whether an individual can safely fly commercial airplanes, it will be difficult for clinicians to determine what information to disclose and then proceed to comb through the record and provide a narrow but fully responsive data set. Providers will thus be tempted or perhaps forced to release the entire EHR to the employer and allow the employer to assimilate the information on its own. To the extent possible, employers will need to develop standardized ways to formulate their medical inquiries. Such standardization may allow EHR vendors to incorporate search and retrieval mechanisms into EHRs that will facilitate standardized modes of response to employer queries. The less burdensome the task of extracting information is for providers, the more likely it is that they will be able to furnish precise and meaningful responses and to follow the HIPAA Privacy Rule principle of limiting disclosures to the minimum necessary for the employer's purposes.[122]

In an electronic age, the ADA's bare-bones requirement that medical information be "maintained on separate forms and in separate medical files"[123] is no longer sufficient to guarantee the confidentiality of health records. Instead, the ADA must require security safeguards for workplace computer systems that store health data. The ADA could reference the HIPAA Security Rule, which itself should be amended to cover employers.[124] In addition, the EEOC could issue guidance to educate employers, many of whom will lack technological sophistication, about how to protect the security of digitized records.[125] Such safeguards are particularly important in light of federal record-keeping regulations that require employers to retain employment-

120. *Id.* § 12112(d)(4)(A).

121. Sharona Hoffman, *Preplacement Examinations and Job-Relatedness: How to Enhance Privacy and Diminish Discrimination in the Workplace*, 49 U. KAN. L. REV. 517, 582 (2001); *see also* Rothstein, *supra* note 4, at 177 (arguing that meaningful protection of genetic information necessitates "the legal requirement to limit the scope of disclosures to job-related information").

122. 45 C.F.R. § 164.502(b)(1 (2009).

123. 42 U.S.C. § 12112(d)(3)(B).

124. *See supra* note 76 (detailing the HIPAA Security Rule's requirements); Part IV.B (formulating recommendations for revision of the HIPAA Privacy and Security rules).

125. *See* Hoffman & Podgurski, *supra* note 76, at 350–54, 370–82 (noting that the HIPAA Security Rule itself lacks sufficient compliance guidance and articulating recommendations to address this concern).

related records for a period of one year from the date of their creation or the personnel action for which they were attained or during the duration of any litigation or administrative proceeding involving the employee at issue.[126] Employers would also be well advised to expunge health records that are no longer needed once the regulatory retention period has expired.

Until the federal government acts, state legislatures could amend state disability laws to provide improved protection to employees and guidance to employers regarding requests for medical records.[127] States that do not limit medical inquiries at all stages of the employment process to those that are job-related should implement this restriction. Furthermore, all states should address the confidentiality of medical records that are stored electronically in the workplace and require employers to implement enhanced security safeguards.

B. Amending the HIPAA Privacy and Security Rules

Because employers routinely handle individually identifiable health information, it is imperative that they be covered by the HIPAA Privacy and Security Rules.[128] These Rules were amended in 2009 to extend to business associates of health insurers, health care clearinghouses, and covered health care providers.[129] However, this modification does not go far enough and does not reach most employers. Inclusion of employers under the scope of the Rules would require employers to comply with all regulatory privacy restrictions, which are more comprehensive and specific than the ADA's general confidentiality mandate. The change would also require employers to implement the security safeguards specified in the regulations if they process individually identifiable health information.[130] This further adjustment to the HIPAA Rules is essential to providing meaningful privacy protections for medical data, which is processed in the workplace with surprising frequency. Likewise, state health information privacy laws should be amended to cover employer conduct if they do not already do so.

---

126. 29 C.F.R. § 1602.14 (2009).

127. *See, e.g.*, *supra* notes 78–81 (providing examples of current state laws addressing disability rights and genetic information).

128. *See* Hoffman & Podgurski, *supra* note 76, at 360–63 (critiquing the HIPAA Security Rule and suggesting means by which it should be strengthened and clarified. Specifically, noting that the term "covered entity" should be expanded to include "'any person who knowingly stores or transmits individually identifiable health information in electronic form for any business purpose related to the substance of such information'").

129. *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13401, 123 Stat. 115 (2009) (explaining that the rules now extend to cover business associates of covered entities).

130. *See supra* Part II.C (explaining HIPAA regulations regarding individually identifiable health information. If the definition were expanded to include employers, they would be required to comply with all HIPAA regulatory requirements).

C. *Technological Improvements and Suitable Government Oversight*

Many of the concerns raised by EHR system use for employees and employers could be addressed through technological improvements and appropriate oversight to ensure the systems' quality. In a rush to install EHR systems in medical practices, policy-makers, vendors, and clinicians cannot neglect the need for interventions that promote the quality, safety and security of all products. Mounting evidence suggests that contemporary products leave much to be desired, and their flaws can have tragic consequences for patients, clinicians, and anyone else who relies on EHRs, including workers and employers.[131]

EHR systems must feature effective query and search capabilities and be able to generate standardized reports for third parties such as employers or litigants. EHR systems should allow for well-organized, comprehensive printouts or PDFs of relevant portions of the patient's records. Technology that facilitates data summarization, cutting and pasting of text, and redaction of documents could enable clinicians to release narrow data sets that are tailored to be responsive to specific employer requests and thus disclose only the minimum necessary information. These steps would enhance patient privacy protections and diminish the likelihood of discrimination.

Advances in system security features and overall quality can also reduce the probability of security breaches that could compromise patient confidentiality. Greater focus on the safety and reliability of systems will reduce medical errors and improve health outcomes, thus reducing the cost of medical care and the expenses of employers who offer health insurance. Improvements that make EHR systems more usable, less cumbersome, and less time-consuming will also ease the transition to computerization for the health care provider workforce.

Such improvements will likely be achieved only with appropriate oversight. The federal government regulates numerous other safety-critical goods and services, including food, drugs, devices, aviation, transportation, and other industries.[132] It is senseless to leave EHR systems, which will manage many aspects of patient care,[133] without meaningful oversight. As the federal government begins to spend billions of dollars to implement health information technology, it must promulgate regulations that establish a careful pre-market approval process and ongoing monitoring of products after they are launched in the marketplace.[134] In addition, federal regulations should specify

---

131. *See, e.g.*, Patrick, *supra* note 116 (focusing on how EHRs impact clinicians); Alexi Mostrous, *Electronic Medical Records not Seen as a Cure-all*, WASH POST, Oct. 25, 2009, at A03 (providing examples of these consequences).

132. *See* Hoffman & Podgurski, *supra* note 3, at 129-30 (discussing government regulation of safety-critical goods and services).

133. *See supra* Part I (explaining the functions of EHRs).

134. *See* Hoffman & Podgurski, *supra* note 3, at 140-64 (articulating recommendations for a regulatory framework for EHR systems).

criteria for system design that optimize product safety and reliability, just as the HIPAA Security Rule details standards and implementation specifications relating to system security.[135]

As the current administration launches its recession-era, multi-billion dollar program to support the adoption of EHR systems, government authorities and the health care community must not become apathetic to the quality of the technology. Detailed regulations and other measures such as agency guidance and carefully formulated clinical practice guidelines can promote optimal EHR system design and use practices.[136] These interventions would benefit all American patients and clinicians as well as others who possess computerized medical records. Suitable oversight and guidance could protect employees whose health data is contained in EHRs as well as employers who must store, process, and assimilate EHR data in order to make responsible employment decisions.

V. CONCLUSION

The sophisticated features and efficiencies of EHR systems have the potential to greatly improve health outcomes and enhance patient welfare. However, this emerging technology also poses significant challenges and risks, not the least of which are its workplace impacts. The breadth of possible disclosures to employers who lawfully seek medical information will intensify workers' concerns about privacy and discrimination. At the same time, usability and readability problems may make it difficult for employers to obtain narrowly tailored information that is relevant and useful for their legitimate purposes. Furthermore, computerized storage of sensitive medical records will likely raise employers' anxiety about security breaches and associated litigation. These concerns can best be addressed through a small number of changes to the ADA, the HIPAA Privacy and Security Rules, and parallel state laws, as well as through technological advances and appropriate federal oversight. As the country transitions to computerization in the medical field, proactive steps must be taken to protect stakeholders in all settings, including the American workplace.

135. *See supra* Part II.C (explaining HIPAA Privacy and Security Rules).

136. *See* Hoffman & Podgurski, *E-Health Hazards*, *supra* note 12.