Washington Journal of Law, Technology & Arts

Volume 3 | Issue 4 Article 4

4-6-2007

Electronic Health Records: Interoperability Challenges Patients' Right to Privacy

Laura Dunlop

ELECTRONIC HEALTH RECORDS: INTEROPERABILITY CHALLENGES PATIENTS' RIGHT TO PRIVACY

Laura Dunlop[1]

Abstract

President George W. Bush's administration has outlined initial necessary steps to transform the healthcare delivery system through adoption of interoperable electronic health records ("EHRs") by the year 2014. This Article examines the nation's shift toward the use of EHR technology, which largely facilitates patient care by providing clinicians with the ability to review a more complete medical record at the time of treatment. Current legislation calls for financial support and technical standards. However, lawmakers neglect to fully address the Health Insurance Portability and Accountability Act ("HIPAA") and the need to expand its application and enforcement. In addition, healthcare provider Anti-Kickback and physician self-referral statutes may continue to deter electronic connectivity progress in healthcare, despite recently finalized safe harbor regulations. The Article concludes that while lawmakers have demonstrated strong support for the health information technology ("HIT") initiatives, significant challenges remain to EHR adoption, including the lack of interoperability standards, financial obstacles, and privacy and security concerns.

Table of Contents

INTRODUCTION

<1> The Bush administration has established a ten-year plan for the nation to implement interoperable[2] electronic health records ("EHRs") by the year 2014.[3] This federal action was in direct response to widespread concern within the healthcare community over the financial and healthcare risks associated with continued reliance on paper-based medical records.[4] The federal government has identified a National Health Information Network (NHIN), made up of Regional Health Information Organizations (RHIOs), as the favored approach to implementing interoperable

EHRs.[5] The network will access and link a series of RHIOs to channel information held in EHRs only to where patients intend for the data to go (e.g., hospitals or physician offices).[6] Two primary goals of the network are to enable consumers to establish and maintain personal health records and to gain greater control over their healthcare outcomes.[7] State governments have entered into a contract with the Department of Health and Human Services' ("DHHS"), Agency for Healthcare Research and Quality and RTI International[8] to assess how privacy and security laws and business practices affect the electronic exchange of health information.[9]

<2> Although there is a strong political push for the nationwide adoption of EHRs, privacy and technology experts have identified several legal challenges to implementation.[10] The move from paper-based records to interoperable virtual records may jeopardize confidentiality and security of personal patient health information. In addition, EHR technology donations to physician practices to facilitate implementation will likely implicate the prohibition of referral relationships under both the Anti-Kickback law and the Medicare physician self-referral (Stark) law.[11] Prerequisites to EHR deployment include the adoption of privacy and security standards and achieving agreement among the primary players (i.e., clinicians, patients, payers) as to consent and disclosure requirements with unreserved respect for patient autonomy.

DISTINGUISHING BETWEEN THE ELECTRONIC HEALTH RECORD (EHR) AND THE ELECTRONIC MEDICAL RECORD (EMR)

<3> There is an important distinction between electronic health records and electronic medical records ("EMRs").[12] EMRs are computerized legal clinical records created within a single healthcare entity. EMRs currently exist in most healthcare practices that have adopted electronic records. A healthcare entity directly provides the medical service and independently owns and maintains the electronic record.[13]

<4> By contrast, the EHR model to which federal and state governments aspire is premised on an aggregation of patient data held in EMRs.[14] An EHR combines personal patient details on health status, information from primary healthcare visitations, and periodic care from other health organizations. The goal with EHRs is to merge a patient's medical history into an electronic record made available on a national level. Thus, regardless of where the patient receives diagnosis or treatment, the health professional has instant access to a comprehensive, updated health record.[15]

<5> Academic and technical literature suggests that EHR implementation could greatly improve healthcare delivery to individual patients. Proponents of EHRs assert that they will increase the quality of care, lower the cost of care and allow for portability of records, while maintaining privacy.[16] EHRs would connect hospital patient data to "downstream" office-based records to transmit clinical data as the patient moves between providers and patient care settings.[17] Interoperable EHRs have the potential to promote access to more detailed and accurate patient information at the time of treatment, reduce medical errors and improve the quality of healthcare.[18]

<6> Some commentators question whether the benefits of EHRs will outweigh inherent risks.[19] There is limited empirical research or analysis regarding how EHRs will improve healthcare. In addition, investigative reports conclude that comprehensive EHRs may not be the best solution. Major obstacles to successful implementation include security and privacy concerns, cost increases[20] , and lack of interoperability.

<7> In particular, the increased flow of electronic information raises a significant concern regarding the privacy and confidentiality of health information. Patient

records, once stored on singular paper documents in locked file cabinets or in EMR entity-controlled electronic format, would instead be stored on multiple computer servers of remotely-connected organizations. This shift to electronic transmission of patient data creates an environment of healthcare data exchange that may be prone to security vulnerabilities as well as human error.[21]

MAJOR FEATURES OF PENDING FEDERAL LEGISLATION

<8> Despite these security concerns the move toward EHRs continues to proceed. Several pieces of proposed federal legislation have key similarities and most address the financial, technical and confidentiality challenges to EHR implementation.[22] The more recent bills include funding provisions to address the high cost of EHR adoption and implementation to physician practices.[23] Further, proposed legislation addresses established prohibitions on physician-hospital relationships.[24] Plans also include some provision for the creation of interoperability, confidentiality and security standards that would support transition to electronic-based record keeping.[25] Overall, there appears to be a consensus within Congress that something needs to be done to provide both technical and financial support for EHR implementation.[26]

<9> Current federal legislative proposals address privacy and security concerns. Some of these bills address the need for patient safety and privacy. Select bills set standards and provisions for the monitoring of technology.[27] Several proposals further attempt to apply the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[28] privacy, confidentiality, and security provisions to health information stored or transmitted in an electronic format. The Bipartisan Health IT Bill, Wired for Health Care Quality Act, for example would plainly establish that current medical privacy rules directly apply to any health information stored or sent electronically.[29] In general, however, legislative attempts to address privacy concerns have not confronted any need for a revision to HIPAA.

STATE-LEVEL EHR INITIATIVES

<10> State and local efforts aimed at creating an interconnected, electronic healthcare system mirror the activities at the national level. Nearly half of the nation's states have issued an executive order or a legislative mandate designed to stimulate the use of HIT. According to the 2006 Third Annual Survey of Health Information Exchange Initiatives and Organizations, sponsored by the eHealth Initiative Foundation (eHI), 28 states have initiated HIT planning and an additional seven states have progressed to the implementation stage.[30] Generally, either a state's governor's office or department of health has assumed leadership in the HIT statewide efforts.[31]

<11> States have assumed an active role in supporting HIT planning and implementation specific to EHR adoption. For example, Arizona Governor Janet Napolitano signed Executive Order 2005-25: Arizona Health-e Connection Roadmap in August of 2005, establishing a steering committee whose goal was to create a "Roadmap" to achieve statewide interoperable EHR adoption. A main objective of the completed Roadmap is the formation of a non-for-profit, public-private partnership to manage statewide health information exchange.[32] In addition, the Minnesota e-Health Initiative, a public-private collaboration, invested considerable funding in HIT deployment including a $1.3 million Minnesota e-Health Initiative Grant Program for Interconnected Electronic Health Records project in statewide rural and underserved areas.[33] Massachusetts launched a pilot educational program to establish EHRs in community-based settings.[34] The conference was part of a several-year-planned project to study the practicality and implications of EHR use in community medical practices.

<12> The Washington State government has also dedicated considerable effort toward developing and implementing a statewide electronic health information infrastructure. The Washington State Health Care Authority's Health Information Infrastructure Advisory Board, supported by a national consultant and the Health Information Infrastructure Stakeholder Advisory Committee, recently delivered a report to the Washington State Legislature summarizing an end vision for statewide availability of health information. The report, representing a broad range of perspectives from Washington's heath care community, identifies how the voluntary system may be developed and operated with significant emphasis on consumer input and control.[35]

LEGAL CHALLENGES TO EHR IMPLEMENTATION

<13> Despite widespread agreement on the inherent benefits resulting from the integration of health information technology, there remain many legal challenges to the sharing of EHRs. The main concerns involve HIPAA's privacy and security regulations, a federal provider Anti-Kickback law, and the Stark anti-referral rules. A patient's right to maintain certain health information confidential poses a significant legal challenge to interoperable EHRs.[36]

Health Insurance Portability and Accountability Act of 1996

<14> HIPAA is the broadest piece of legislation regulating confidentiality and security of patient care data among the numerous federal laws addressing the use of health information.[37] Through its administrative regulations, collectively known as the HIPAA Privacy Rule, the statute established a set of basic federal guidelines to limit the use and disclosure of "protected health information" ("PHI")[38] to allow for necessary patient information flow between healthcare providers.[39] HIPAA does not directly protect patient privacy, but rather places *confidentiality*-based limitations on information provided to healthcare entities.[40] HIPAA covers any form of PHI information including information electronically maintained and transferred. HIPAA, however, does not address specific EHR-related privacy and security concerns.[41]

<15> Despite its protections for personal health information, privacy experts warn that HIPAA does not fully anticipate the government's model of unrestricted sharing of information among a wide network of unrelated healthcare providers.[42] The standards present a challenge to the federal government's plan for EHR deployment, where completely unrelated clinicians can request, locate, and obtain patient medical records. Additionally, there exists the challenge of maintaining appropriate security safeguards for information sharing to ensure the integrity of patient-related content.[43] Consequently, EHRs could create the potential for privacy violations on an unprecedented scale.[44]

<16> Moreover, HIPAA directly covers only a core group of "covered entities" that hold and maintain healthcare information and their "business associates" who assist with certain business processes.[45] As the DHHS noted, many of the people and organizations that receive, use, and disclose protected health information remain outside the system of federal regulation because they are not involved in the business processes covered by HIPAA.[46] For example, HIPAA does not cover businesses that provide health information services to customers over the Internet.[47] Additionally, workers compensation carriers, researchers, life insurance issuers, employers, and marketing firms fall beyond the scope of HIPAA.[48] Furthermore, DHHS lacks authority to impose civil or criminal penalties against "business associates."[49]

<17> Any EHR vendor that purposefully or incidentally interacts with PHI in

developing an EHR, or providing support services, would be categorized as a business associate.[50] Similarly, DHHS may lack the ability to directly regulate employees of covered entities who obtain or disclose PHI.[51] Consequently, without adequate federal privacy protections, federal efforts to create a national health information network through EHR deployment pose a challenge to patient privacy.

<18> The privacy of health information has become a fundamental concern as the shift toward electronic exchange of health information and EHR deployment continues.[52] Some commentators suggest that Congress consider expanding HIPAA privacy protections to ensure that health information use and disclosure standards apply to all entities that receive or generate PHI.[53] Experts recommend, for example, that the HIPAA Rules subject to legal sanction not only providers, health plans, and clearinghouses, but also those "business associates" whose access to personal health information will only continue to increase with EHR implementation.[54] These commentators further advise that a federal private cause of action would deter those who intentionally and improperly obtain, use and disclose health information by subjecting them to civil and criminal penalties.[55] To date, Congress has not enacted legislation to address these privacy concerns.

Prohibitions on Referrals for Compensation: Stark and Anti-Kickback Laws

<19> The federal Anti-Kickback and Stark laws present additional challenges to EHR implementation, because both prohibit donations in exchange for physician referrals in most cases.[56] The Stark "physician self-referral" law prohibits physicians that have entered into a financial relationship with a healthcare entity from making certain patient referrals to that entity.[57] The Stark law was specifically designed to facilitate referrals between hospitals and referring physicians, and therefore will likely have an effect on EHRs. For example, there would be a potential breach of the Stark Act if a hospital and doctor entered into an arrangement whereby the hospital supplies equipment or financial support to the doctor as a condition of granting access to the EHR network.[58]

<20> The Stark law contains two limited exceptions applicable to interoperable EHR technology.[59] First, "wholly dedicated hardware" is not "remuneration."[60] Therefore, there would be no Stark violation if a hospital provides a physician practice with computer hardware to access their EHR system under strict agreement to limit use to solely patient-related purposes. In addition, a Stark exception protects "remuneration" in the form of hardware and software used in the case of "community-wide health information systems," assuming both parties strictly adhere to specific qualifications.[61] Experts question whether the term sufficiently covers the range of various health IT arrangements.

<21> The federal Anti-Kickback statute similarly imposes criminal liability for the knowing and willful payment, solicitation, or receipt of donations in return for referring patient services reimbursable by a federal healthcare program (e.g., Medicare, Medicaid).[62] There is valid concern that the donative value will incline physicians to refer business back to the hospital in exchange for the in-kind value of the technology when a hospital arranges to grant access to its EHR by offering costly equipment and software to its medical staff.[63]

SAFE HARBOR SOLUTIONS TO EASE THE FINANCIAL BARRIER AND PROTECT HEALTH PROVIDERS FROM PROSECUTION

<22> The Stark and Anti-Kickback laws provide protection against federal fraud and abuse. The laws do not, however, directly address current-day HIT arrangements.[64] In drafting those laws, Congress did not anticipate interoperable EHRs that

necessarily involve downstream relationships among different providers in different care settings. As a result of the uncertainty surrounding legal consequences, healthcare providers remain reluctant to invest in costly HIT. Therefore, the CMS and the Office of Inspector General ("OIG") recently finalized safe harbors to more broadly allow for permissible in-kind provision of technology tools to affiliated physicians by hospitals and other suppliers to encourage EHR adoption without creating inappropriate conflicts of interest or potential for abuse.[65]

<23> CMS has adopted a final EHR Stark safe harbor[66] that protects business arrangements involving the provision of software, information technology, or training services "necessary and *used predominately*[67] to create, maintain, transmit, or receive electronic health records" (e.g. connectivity, maintenance services, and help desk support).[68] Hardware donations are not protected under the safe harbor. CMS expanded the Stark protections to cover all entities that provide designated health services as protected donors and any physician as a permissible recipient.[69] Whereas the Stark exception encourages legitimate technology donations, it precludes protection where the donor either knows that the recipient physician already owns equivalent technology or acts in deliberate ignorance or reckless disregard of that fact.[70] Consistent with the President Bush's goal of EHR implementation by 2014, all donations of EHR technology must occur, and conditions for protection must be satisfied, on or before December 31, 2013.[71]

<24> The DHHS OIG has adopted the same sunset provision and nearly identical conditions for EHR Anti-Kickback protection as provided for under the Stark safe harbor.[72] The finalized EHR Anti-Kickback exception similarly loosens legal restrictions to allow EHR-related software and training services donations without violating federal fraud and abuse laws.[73] It specifically protects arrangements involving EHR technology donations by health plans or providers that submit claims or requests for payment to a federal healthcare program to individuals or entities engaged in the delivery of healthcare. The Anti-Kickback safe harbor additionally bars donors from shifting costs to federal healthcare programs.[74]

<25> Overall, experts anticipate that these final safe harbors will encourage wider adoption of digital health records while better protecting healthcare providers from prosecution.[75] However, concerns remain that provision of HIT to physicians by hospitals could implicate the Anti-Kickback and anti-referral laws. In addition, experts foresee disagreement on the interpretation of certain requirements in the final rule, such as how a donor is to calculate EHR implementation costs to accurately allocate fifteen percent of the donor's cost of the technology to the recipient.

ADDITIONAL MEASURES TO MITIGATE THE RISKS

<26> Legislative safeguards and appropriate security measures to protect the confidentiality of the patient medical record must accompany ongoing advancements in the interactive network environment. Experts recognize that when the government attempts to address issues of technology, "technology often outpaces the legislation."[76] Therefore, policymakers must engage the IT community in the legislative and planning process. If carefully implemented, with comprehensive input from the necessary players, EHRs will serve as a quality tool to improve healthcare delivery while maintaining patient privacy.[77]

<27> The DHHS recognizes that the success of the American healthcare system depends largely upon the willingness of individuals to openly share their most private medical concerns with their healthcare providers.[78] However, recent reports indicate that the public perceives the "increasing use of interconnected electronic information systems as one of the greatest threats to medical privacy."[79] A key area of debate centers on the requirement that a patient consent before providers include

information in an EHR and/or disclose the protected data to others through the EHR network. Privacy proponents argue that by giving patients a choice in this regard, individuals maintain a degree of control directly in line with the national trend toward healthcare consumer empowerment.[80] However, physicians counter that patient control over files may actually hinder the quality of care provided. Policymakers will need to balance the interests of patients and providers, emphasizing the importance of patient autonomy.[81]

CONCLUSION

<28> Although EHR technology largely facilitates patient care by providing clinicians with the ability to review a more complete medical record, interoperability and privacy issues present significant barriers to implementation of the EHR. Current legislation identifies the importance of financial support and technical standards. However, these bills neglect to address the need to expand HIPAA's scope to cover downstream entities that are given access to protected health information and to provide for a private cause of action. With the ability to review a more complete medical record, interoperability and privacy issues present significant barriers to implementation of EHRs. The final Stark rule and Anti-Kickback safe harbors potentially remove certain obstacles to successful implementation. For example, the proposals will likely facilitate a shift in costs of EHR adoption from physicians and small providers to more financially sound hospitals and other payers. However, experts express concern over the interpretation and application of the arguably vague provisions. EHR implementation is inevitable due to the breadth of support from healthcare regulators, hospital administrators, payers, and physician advocacy groups. If properly funded and carefully implemented, EHRs will transform healthcare delivery while maintaining the integrity and privacy of patient information.

PRACTICE POINTERS

- Even if EHRs cannot fully comply with the safe harbor requirements, the organization should structure any venture to meet as many of the current Anti-Kickback safe harbor elements as possible to reduce risks.
- Healthcare providers contemplating EHR adoption should "plan and negotiate for the long-term and a changing environment; anticipate evolving operations, emerging technologies, new laws and the long-term obsolescence of whatever the entity may implement."[82]
- In the development of EHR contracts, healthcare entities and providers should research whether the adopted EHR system will be certifiable, meet federal data standards, and meet best security practices and standards.[83]
- Healthcare providers must clearly define permitted and prohibited uses of PHI in the contract terms for those EHR vendor business associates with access to patient data, as needed for development or support only.

<< Top

Footnotes

1. Laura Dunlop, University of Washington School of Law, Class of 2007. Thank you to the Shidler editorial student staff, University of Washington Professor Anita Ramasastry and John R. Christiansen of Christiansen IT Law for their greatly appreciated contributions to this Article.
2. The objective of interoperability is to "support the electronic exchange of

patient summary information among caregivers and other authorized parties via EHR systems. . . to improve the quality, safety, efficiency, and efficacy of care delivery." An EHR that is interoperable allows for different EHR systems to exchange patient summary information with greater ease and at less cost by establishing universal user standards and supporting more complex requirements for future data exchange. HIMSS EHR VENDOR ASS'N, WHITE PAPER ON INTEROPERABILITY 1 (2005), http://www.himssehrva.org/docs/EHRVAExpandedPositionStatementfinal042905.pdf .

3. KELLY CRONIN, DEP'T OF HEALTH & HUMAN SERVS., THE DECADE OF HEALTH INFORMATION TECHNOLOGY: FRAMEWORK FOR STRATEGIC ACTION 3 (2004), https://www.clinicalresearchnetworks.org/documents%5CJune%201%5CKeynote%20Speech . A full definition of the EHR is provided in the subsequent section entitled "Distinguishing between the Electronic Medical Record (EMR) and the Electronic Health Record (EHR)."

4. Risks originally identified in the 1999 Institute of Medicine report on medical errors. LINDA T. KOHN ET AL., TO ERR IS HUMAN: BUILDING a SAFER HEALTH SYSTEM (Janet Corrigan et al. eds., National Academies Press 2000). President Bush issued Executive Order 13335, creating the Office of National Coordinator for Health Information Technology ("ONCHIT") in order to develop a federal government-wide strategy for adopting health information technology. The ONCHIT aims to better inform clinical practice by "bringing information tools to the point of care, [specifically] by investing in EHR systems in both physician offices and hospitals." TOMMY G. THOMPSON & DAVID J. BRAILER, DEP'T OF HEALTH & HUMAN SERVS., FRAMEWORK FOR STRATEGIC ACTION: THE DECADE OF HEALTH INFORMATION TECHNOLOGY - DELIVERING CONSUMER-CENTRIC AND INFORMATION-RICH HEALTH CARE (2004), http://www.hhs.gov/healthit/documents/hitframework.pdf.

5. U.S. DHHS, Office of the National Coordinator for Health Information Technology GOALS OF STRATEGIC FRAMEWORK (2004), http://www.hhs.gov/healthit/goals.html.

6. *Id.*

7. *Id.*

8. RTI International is a private research institute that offers research and technical solutions to governments and businesses worldwide.

9. *Id.*

10. *See* Interoperable Electronic Health Records Task Force, American Health Lawyers Assoc., The Quest for Interoperable Electronic Health Records: A Guide to Legal Issues in Establishing Health Information Networks (2005).

11. Both laws are intended to counter fraud and abuse. The federal Stark Law prohibits a physician from referring Medicare patients for certain patient services to an entity with which the physician has a financial relationship, unless an exception applies. EHR hardware or software directly or indirectly funded by, for example, a hospital or health system to enable access to the EHR network would create a financial relationship and thus violate the Stark Law. 42 U.S.C. § 1395nn (2000). The Anti-Kickback statute prohibits the payment or solicitation, offer, or acceptance of any remuneration in cash or kind in exchange for referring or recommending the referral of items or services to be paid by a federal healthcare benefit program (e.g., Medicare, Medicaid). *See* 42 U.S.C. §

1320a-7b(b) (2000).

12. DAVE GARETS & MIKE DAVIS, HEALTHCARE INFORMATICS ONLINE, ELECTONIC PATIENT RECORDS: EMRS AND EHRS 1-2 (2005), http://www.providersedge.com/ehdocs/ehr_articles/Electronic_Patient_Records-EMRs_and_EHRs.pdf.

13. *Id.*

14. However, a system-wide EMR maintained by a largely integrated provider would potentially contain data similar to that found in a longitudinal EHR. A longitudinal record combines information about patient contacts with primary healthcare as well as subsets of information associated with the outcomes of periodic care. *Id.*

15. *See* Health Information and Management Systems Society (HIMSS), Electronic Health Record, http://www.himss.org/ASP/topics_ehr.asp (last visited February 26, 2007).

16. Letter from the Board on Health Care Services, Institute of Medicine to the Agency for Healthcare Research and Quality (July 31, 2003).

17. *Id.*

18. em> Id.

19. Jaan Sidorov, *It Ain't Necessarily So: The Electronic Health Record and the Unlikely Prospect of Reducing Health Care Costs*, 25 HEALTH AFFAIRS No. 4 1079 (2006), *available at* http://content.healthaffairs.org/cgi/content/full/25/4/1079. *See also* Kate Ackerman, *Study: EHR Adoption Predicted Not to Meet 2014 Goal*. IHEALTH BEAT, Jan. 10, 2006, http://www.ihealthbeat.org/index.cfm?Action=dspItem&itemID=117987.

20. EHR start-up and maintenance costs present a significant financial challenge to successful implementation. The average cost of an EHR ranges from $16,000 to $36,000. Patrick Stokes, *Privacy and Security Issues of a National Health Information Network*, 9 J. ENG'G & PUB. POL'Y, Aug. 2002, *available at* http://www.wise-intern.org/journal/2005/Stokes.pdf. Thus, many small physician practices do not have the capital budget available for EHR technology acquisition. Moreover, the patients, not the providers who bear the implementation costs, benefit from the improved practice efficiency and increased quality of care. *See also* Kate Ackerman, *Study: EHR Adoption Predicted Not to Meet 2014 Goal*, IHEALTH BEAT, Jan. 10, 2006,http://www.ihealthbeat.org/index.cfm?Action=dspItem&itemID=117987.

21. Unintentional disclosure threatens confidentiality of health information in electronic format. For example, several thousand electronic patient records at the University of Michigan Medical Center, including names, job status, treatment information, and other personal data, were inadvertently posted on public Internet sites for two months. *Black Eye at the Medical Center*, WASH. POST, Feb. 22, 1999, at F5. The opportunity for improper access and disclosure of electronic medical records by health institution employees also poses significant risk. Recently, an employee of a cancer clinic accessed the medical records of a terminal cancer patient, obtained credit cards in the patient's name, and charged over $9000 in personal purchases. Press Release, U.S. Attorney's Office, Western District of Washington, Seattle Man Pleads Guilty in First Ever Conviction for HIPAA Privacy Rules (Aug. 19, 2004) (on file with author). Additionally, many employees within a healthcare organization access and disclose medical information out of curiosity. An employee at a major

hospital in Washington, D.C. improperly accessed a co-worker's medical record to discover and later reveal the patient's HIV status. P. Slevin, *Man Wins Suit Over Disclosure of HIV Status*, WASH. POST, Dec. 30, 1999, at B4.

22. *See* HIMSS, HIMSS Federal HIT Legislative Crosswalk, updated Sep. 22, 2006, http://www.himss.org/advocacy/news_crosswalk.asp.

23. The Health Information Technology Act of 2005, S. 1227, 109th Congress (*available at* http://www.thomas.gov).

24. *See* 21st Century Health Information Act of 2005, H.R. 2234, 109th Congress; Health America Act of 2005, S. 1503, 109th Congress.

25. *See, e.g.*, Information Technology for Health Care Quality Act, S. 2907, 108th Congress; Patient Safety and Quality Improvement Act, H.R. 663, 108th Congress; 21st Century Health Information Act of 2005, H.R. 2234, 109th Congress.

26. Representative Patrick Kennedy and Representative Tim Murphy sponsored the 21st Century Health Information Act. Senator Hillary Rodham Clinton and then-Senate majority leader Dr. Bill Frist also introduced the Health Technology to Enhance Quality Act of 2005 (or the "Health TEQ Act" S. 1262). Several recently introduced federal bills have sought to provide incentives for EHR adoption and accelerate the development of data interoperability. For example, the Health Information Technology Act of 2005 would provide $4.05 billion over 5 years in federal grants to healthcare providers to assist in the acquisition or lease of health informatics hardware and software. Grant recipients (e.g. hospitals and physicians) would be required to comply with the intended HHS "voluntary" standards on interoperability, as established in the same bill. *See* Health Information and Management Systems Society (HIMSS), HIMSS Federal HIT Legislative Crosswalk, updated Sep. 22, 2006, http://www.himss.org/advocacy/news_crosswalk.asp. Considerable concerns exist over the financial support for nation-wide EHR implementation. While the Bush administration strongly promotes adoption of health information technology, consultants note that the proposed level of funding is inadequate to achieve the government's objective. PRICEWATERHOUSE COOPER'S HEALTH RESEARCH INSTITUTE, PRESIDENT BUSH'S SECOND TERM: PRESCRIBING PRIVATE SOLUTIONS FOR THE NATIONS' HEALTHCARE PROBLEMS (2004). In response, legislative proposals identify a variety of financing options to incentivize rather than mandate EHR adoption. *Id.*

27. *See* Patient Safety and Quality Improvement Act of 2005, S. 544, 109th Congress.

28. Health Insurance Portability and Accountability Act of 1996 ("HIPPA"), 42 U.S.C. § 201 (2000); *see also* HIPAA Privacy Rule, 45 C.F.R. §§ 160, 164.500-164.534 (2006).

29. The Wired for Health Care Quality Act (S. 1418) was the combination of two previously-proposed bills: the Health Technology to Enhance Quality Act of 2005 (S. 1262) and the Better Healthcare Through Information Technology Act (S. 1355). The bill was sponsored by four political leaders: Sen. Hillary Rodham Clinton (D-NY), Senate Majority Leader Bill Frist (R-TN), Sen. Edward Kennedy (D-MA) and Sen. Michael Enzi (R-WY). The legislation, developed to help establish ONCHIT forms a process for adopting healthcare IT standards, authorizing grants and setting quality standards. As part of The Healthy America Act of 2005 (S. 4), Frist also proposes a HIPAA study (study of state laws).

30. For up-to-date information on individual state Healthcare IT initiatives *see* http://www.hitdashboard.com/MapPage.aspx.

31. EHEALTH INITIATIVE, STATES GETTING CONNECTED: QUALITY AND SAFETY DRIVING HEALTH IT PLANNING IN A MAJORITY OF THE STATES IN THE UNITED STATES 1 (2006), http://www.ehealthinitiative.org/assets/documents/eHI2006ReportonStateActivities.pdf#search=%22state%20initiatives%20%22electronic%20health%20record%22%202006%22 .

32. Arizona has budgeted $1.5 million to establish grants in promotion of HIT adoption and additionally was awarded a $350,000 federal grant to explore e-Health privacy and security issues. *Id.*

33. *Id.*

34. The one-day conference entitled "EHR in Your Office – Let's Get Started" is sponsored by the Massachusetts e-Health Collaborative, the Massachusetts Medical Society in Waltham, and the Healthcare Information and Management Systems Society (HIMSS). Healthcare Information and Management Systems Society, *Massachusetts takes a giant step toward electronic health records*, Oct. 5, 2006, http://www.himss.org/ASP/topics_News_item.asp?cid=65349&tid=9.

35. The Board recommends an initial state investment of $8 million to $11 million for design work, $4 million to $5 million in the form of grants to subsidize implementation costs, and $1 million to $2 million to support adoption efforts by the Washington Health Information Collaborative program over the next two years. WASHINGTON STATE HEALTH CARE AUTHORITY, WASHINGTON STATE HEALTH INFORMATION INFRASTRUCTURE: FINAL REPORT AND ROADMAP FOR STATE ACTION [page #] (2007), http://www.hca.wa.gov/hit/doc/finalreport.pdf.

36. Stark exceptions fall into three categories based on the type of financial relationship between the physician and the entity to which he refers patients. (1) Exceptions applicable to both compensation and ownership/investment arrangements (e.g., in-office ancillary services); (2) Exceptions applicable to ownership or investment arrangements (e.g. publicly-traded securities and mutual funds, or ownership in a hospital); (3) Exceptions applicable only to compensation arrangements (e.g., employment relationships or rental of office space or equipment). 42 C.F.R. § 411.357 (2006).

37. Health Insurance Portability and Accountability Act of 1996 ("HIPPA"), 42 U.S.C. § 201 (2000); *see also* HIPAA Privacy Rule, 45 C.F.R. §§ 160, 164.500-164.534 (2006).

38. HIPAA generally defines Protected Health Information (PHI) as any "individually identifiable health information." 45 C.F.R. § 160.103 (2006).

39. The HIPAA Privacy Rule covers applicability, individual rights, permitted uses and disclosures with and without consent, information practices, preemption, enforcement, and penalties. 45 C.F.R. §§ 160, 164.500-164.534 (2006).

40. An objective of the HIPAA Privacy Rule is to ensure *confidentiality* (as opposed to privacy), integrity and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits. It is important to understand the difference between privacy and confidentiality: Privacy refers to a person's desire to control and limit the access of others to themselves or to information about themselves. In contrast, confidentiality refers to the treatment of identifiable, private

information that has been disclosed to others, usually in a relationship of trust, with the expectation that it will not be shared except in ways that have been previously agreed upon. *See* Educause.edu, http://www.educause.edu/Browse/645?PARENT_ID=547 (last visited Jan. 7, 2007). The Privacy Rule allows uses and disclosures of PHI for treatment, payment, and oversight (e.g. management and administrative supportive activities) by covered entities without patient pre-approval. All other disclosures require prior written authorization. HIPAA covers any form of PHI information including information electronically maintained and transferred. Covered entities include health plans, healthcare providers, and healthcare clearing houses. 45 C.F.R. §§ 160, 164.500-164.534 (2006).

41. Christine Kilgore, *Electronic Medical Records Put New Focus on Accuracy (Practice Trends)*, INTERNAL MED. NEWS, April, 2005, http://www.findarticles.com/p/articles/mi_hb4365/is_200504/ai_n15252242 .

42. Edward F. Shay, *Legal Barriers to Electronic Health Records*, PHYSICIAN'S NEWS DIGEST, May 2005, *available at* http://www.physiciansnews.com/law/505.html.

43. The HIPAA Security Rule requires covered entities (i.e. health plans, healthcare providers, and healthcare clearinghouses) to secure PHI against any reasonably anticipated threats or unauthorized uses. The Security Rule's requirements are organized into three categories: administrative safeguards, physical safeguards, and technical safeguards. Within these categories are eighteen specific standards that constitute required protection. The nine administrative standards address organizational measures necessary to better manage and secure the day-to-day operations (i.e. implementation of security policies and procedures, prevention and detection of security intrusions, employee information security training sessions). The four physical standards require covered entities to limit physical access while allowing properly-authorized access (i.e. restriction on data access by use of locks, workstation security and implementation of controls on movement of workstation hardware). The five technical safeguards focus on procedures designed to protect computer system integrity (i.e. policy and procedure implementation to: restrict access to approved users, regularly audit the information, protect the information from corruption, authenticate user accessing the data, and protect personal information in transmission). *See* 45 C.F.R. §§ 164.304-312 (2006); for a more complete list *see* U.S. DEP'T OF HEALTH & HUMAN SERVICES, HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) COMPLIANCE GUIDE 14-18 (2005), http://csrc.nist.gov/fasp/FASPDocs/program-mgmt/HHS_HIPAA_Compliance_Guide_09142005.pdf (last visited Feb. 22, 2007).

44. Media reports suggest that despite HIPAA protections, U.S. privacy and security of patient health information is lacking. For example, 2005 reports included stolen laptop computers containing medial information, theft of a computer disk which contained medical and financial information for 200,000 patients, hacking of health information technology, and a disaffected employee linking her personal weblog to the medical information of 140 patients. Moreover, identity thieves have regularly targeted healthcare facilities because of the relative exposure of social security numbers and other personal data. Kevin Helliker, *A New Medical Worry: Identity Thieves Find Ways to Target Hospital Patients*, WALL ST. J., Feb. 22, 2005, at D1.

45. A "business associate" is defined under HIPAA as any entity that obtains or uses protected health information (PHI) on behalf of a covered entity. The following business processes are covered when performed by a business association: administrative, legal, accounting, consulting, data aggregation, management, accreditation, or financial services. 45 C.F.R. §§ 164.103-.105 (2006).

46. For example, HIPAA covers only those providers who transmit health information electronically for certain administrative or financial purposes. *Id.*

47. Centers for Medicare & Medicaid Services provides public access to an electronic support tool to assist in determining whether an entity qualifies as a covered entity under HIPAA. CTR FOR MEDICARE & MEDICAID SERV, ARE YOU A COVERED ENTITY? http://www.cms.hhs.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp#TopOfPage (last visited Feb. 22, 2007).

48. *Id.*

49. *See* 45 C.F.R. §§ 160, 164.500-164.534 (2006).

50. *See* 45 C.F.R. § 160.103 (2006).

51. The U.S. Department of Justice has recently taken the position that criminal penalties generally apply only to entities and not to those individual employees who illegally or improperly obtain and use health information. Memorandum from the Office of Legal Counsel to the General Counsel Dep't of Health & Human Services and the Senior Counsel to the Deputy Attorney Gen. 2005 WL 2488049 (O.L.C.) (Pre. Print) (June 1, 2005), *available at* http://www.usdoj.gov/olc/hipaa_final.htm. *But see* Press Release, U.S. Attorney's Office S. D. Fla., Two Charged in Computer Fraud, Identity Theft and Health Care Fraud Conspiracy (Sept. 8, 2006), *available at* http://miami.fbi.gov/dojpressrel/pressrel06/mm20060908.htm (Cleveland Clinic employee allegedly downloaded patient files and sold patient information to cousin who used data to submit approximately $2.8 million in fraudulent Medicare claims). Defendants have been charged on multiple counts, including violation of HIPAA, 42 U.S.C. § 1320d-6(a)(2) (2000). At the time, the HIPAA prosecution was the first of its kind in the Southern District of Florida, and the third in the nation.)

52. Pam Dixon, *Electronic Health Records and the National Health Information Network: Patient Choice, Privacy, and Security in Digitized Environment*, WORLD PRIVACY FORUM, Aug. 16, 2005, *available at* http://www.worldprivacyforum.org/testimony/NCVHStestimony_092005.html .

53. Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617 (Spring 2002).

54. *Id.*

55. *Id.*

56. 42 U.S.C. § 1320a-7b(b) (2000); 42 U.S.C. § 1395nn (2000).

57. 42 U.S.C. § 1395nn (2000).

58. Shay, *supra* note 42.

59. 42 U.S.C. § 1395nn.

60. *Id.* Privacy experts interpret remuneration to mean donations in-kind. Shay, *supra* note 42.

61. These qualifications include (1) a requirement that hardware and software be necessary in order to participate in the community-wide health information system; (2) suppliers of technology and support cannot take referrals into account in terms of whether a (business associate?) does or does not receive support; and (3) any community-wide system must be available to all providers who wish to participate in the system. Shay, *supra* note 42.

62. 42 U.S.C. § 1320a-7b(b) (2006).

63. Shay, *supra* note 42.

64. Researchers at RTI International are working in collaboration with the Office of the National Coordinator for Health Information Technology to establish standards aimed at improving claims accuracy and the detection of fraudulent claims submitted against public and private health care plans. The standards will be recommended for use in EHR systems. The recommendations are available for public review through site registration at http://ehrantifrauddev.rti.org. *See* RTI International, *Researchers Seek Comments on Recommendations Designed to Improve Efficiency, Prevent Health Fraud*, Dec. 21, 2006, http://www.rti.org/newsroom/news.cfm?nav=442&objectid=99D16F1F-056C-4E68-88794DEF6482F3B4 for additional information.

65. Letter from Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C. to the Office of Inspector General, Centers for Medicare and Medicaid Services (Feb. 8, 2005).

66. 42 C.F.R. § 411.357(w) (2006).

67. Emphasis added. The EHR protections apply a "used predominately" standard as an alternative to the "used-solely" standard found in the e-prescribing Stark protections. Health Law & Business Library, *OIG, CMS Issue Final Anti-Kickback and Stark Protections For E-Prescribing and EHR Arrangements* (Aug. 9, 2006), *available at* http://www.bna.com/press.

68. The receiving provider must independently finance fifteen percent of the donor's cost for the item or services prior to receipt. The cost sharing requirement must be documented in a written agreement. 42 C.F.R. § 411.357(w) (2006).

69. Selection criteria to identify qualified physician recipients, deemed not to be directly related to the volume and value of referrals generated, now additionally includes (1) whether the physician is on the donor's medical staff and (2) the level of uncompensated care provided. *Id.*

70. *Id.*

71. *Id.*

72. Health Law & Business Library, *OIG, CMS Issue Final Anti-Kickback and Stark Protections For E-Prescribing and EHR Arrangements* (Aug. 9, 2006), *available at* http://www.bna.com/press.

73. *Id.*

74. *Id.*

75. Richard Saunders & Amy L. Young, *New Stark Law Exception and Anti-Kickback Statute Safe Harbor for E-Prescribing and Electronic Health Record Technology*, Mondaq Business Briefing, Aug. 23, 2006, http://www.mondaq.com/article.asp?articleid=42200.

76. Cayce D. Utley, *Federal Activity on Implementation of Electronic Health*

Records (EHRs), CENTRIST.ORG, Sept. 9, 2004, http://www.centrists.org/pages/2004/09/1/ehr.html.

77. The public-private Markle Foundation's Connecting for Health Common Framework provides a comprehensive online resource for implementing private and secure health information exchange. Connectingforhealth.org, The Connecting for Health Common Framework, http://www.connectingforhealth.org/commonframework/index.html (last visited Jan. 7, 2007).

78. 65 Fed. Reg. 82,467 (Dec. 28. 2000).

79. 65 Fed. Reg. 82,474.

80. OFFICE OF THE FEDERAL PRIVACY COMMISIONER, HEALTH*CONNECT* INTERIM RESEARCH REPORT AND DRAFT SYSTEMS ARCHITECTURE 3 (2004), http://www.privacy.gov.au/publications/healthcsub04.doc.

81. Experts suggest that patients will need to maintain some control over their personal health information by, for example, placing certain individual restrictions on inclusion and disclosure of information. In addition, physicians likely will need to be more open to patient request to alter their medical records or make a conscious effort to review the record's content together during patient visits. Kilgore, *supra* note 41.

82. Audio conference: EHR Prep: How to Negotiate Your Contract, held by HCPro John Christiansen & Richard Marks (March 21, 2006) (on file with author).

83. *Id.* at 13.