Viewpoint

The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions

Tracy D Gunter[1], MD; Nicolas P Terry[2], LLM

[1]Department of Psychiatry, Roy J. and Lucille A. Carver College of Medicine, University of Iowa, Iowa City, IA, USA
[2]Center for Health Law Studies, School of Law, Saint Louis University, St. Louis, MO, USA

Corresponding Author:
Nicolas P Terry, LLM
Center for Health Law Studies
School of Law
Saint Louis University
3700 Lindell Boulevard
St. Louis, MO 63108
USA
Phone: +1 314 977 3998
Fax: +1 314 977 3332
Email: terry@slu.edu

Abstract

Emerging electronic health record models present numerous challenges to health care systems, physicians, and regulators. This article provides explanation of some of the reasons driving the development of the electronic health record, describes two national electronic health record models (currently developing in the United States and Australia) and one distributed, personal model. The US and Australian models are contrasted in their different architectures ("pull" versus "push") and their different approaches to patient autonomy, privacy, and confidentiality. The article also discusses some of the professional, practical, and legal challenges that health care providers potentially face both during and after electronic health record implementation.

(J Med Internet Res 2005;7(1):e3) doi: 10.2196/jmir.7.1.e3

KEYWORDS

Medical records systems, computerized; delivery of health care; patient care; information management; medical record linkage; confidentiality; policy making; United States; Australia; Internet

Introduction

The electronic health record (EHR) is an evolving concept defined as a longitudinal collection of electronic health information about individual patients and populations. Primarily, it will be a mechanism for integrating health care information currently collected in both paper and electronic medical records (EMR) for the purpose of improving quality of care. Although the paradigmatic EHR is a wide-area, cross-institutional, even national construct, the electronic records landscape also includes some distributed, personal, non-institutional models.

Emerging EHR models present numerous challenges to health care systems, physicians, and regulators. This article provides explanation of some of the reasons driving the development of the EHR, describes three different EHR models, and discusses some of the practical and legal challenges that health care providers potentially face both during and after EHR implementation.

Stakeholders and Drivers

Information technology (IT) has become the principal vehicle that some believe will reduce medical error. In the United States, the non-governmental and highly influential Institute of Medicine (IOM) has committed to technology-led system reform [1] and urged "a renewed national commitment to building an information infrastructure to support health care delivery, consumer health, quality measurement and improvement, public accountability, clinical and health services research, and clinical education." [2] As is well known, this IT-led system reform involves several intersecting technologies, including the following: tracking systems (barcodes and Radio Frequency Identification [RFID]); computerized physician order entry (CPOE) systems; clinical decision support systems (CDSSs) that complement order entry devices operating with server-side systems that reference drug interaction information or treatment models (such as clinical practice guidelines); and enhanced reporting systems that provide for adverse event and medical

error disclosure, and facilitate population-based health care models and more extensive outcomes research.

The electronic record is at the center of the IOM's goal of eliminating most handwritten clinical data by the end of this decade [2]. Electronic records are superior to paper records because they decrease error due to handwriting problems and ease physical storage requirements [3]. Additionally, electronic records simultaneously leverage other error-reducing technologies and render them coherent. EHR models present significant additional advantages because of their potential to deliver a longitudinal record that tracks all medical interactions by a particular patient and provide comprehensive data across populations. Thus, the IOM envisions a longitudinal collection of electronic health information for and about individuals and populations as feeding data into error-reducing "knowledge and decision support systems." [4,5]

Error reduction aside, business concerns and structural changes in health care delivery are driving EHR implementation. Although some of these phenomena are unique to the US model of health care financing and delivery, mature systems in other countries must also accommodate stresses from similar developments. First, the shift from in-patient to ambulatory care (and other episodic models) has accelerated the need for accurate and efficient flow of patient medical and billing information between organizationally and geographically distinct providers. Second, the operational aspects of managed care, such as the data needs of "gate keeping" physicians, demands by payers for performance "report cards," and system administrators' increasing needs for sophisticated utilization review and risk management tools, have increased the need for data transparency [6]. Third, the growth of "shared care", whereby the patient both shares responsibility with the provider for care and is likely to have increasingly fragmented or episodic relationships with multiple providers, requires that patients must have access to health data generally and, more controversially, to information in their record [7,8]. Furthermore, it requires that providers have transparent access to other occasions of treatment, particularly pharmacotherapy. Finally, both patients and regulators are demanding increasing amounts of data regarding errors or near misses and outcomes in populations [9]—data that is difficult to generate without sophisticated data coding and nearly impossible to analyze without complex, comprehensive database systems.

In addition to safe, high-quality care, patients expect privacy, rights of access and correction [7], and the opportunity to give consent for research uses of their health information [10]. As patient care moves from an in-patient to ambulatory or other fragmented models of service delivery utilizing multiple providers, the portability of and timely access to data become increasingly important to patients as well as providers. In the words of one patient,

> *I don't want much - just for my medical records to be seen only by those whom I authorize, and for the record to be readily accessible to them wherever they are. . . . I would like a bigger say in what goes into my notes, and if I don't like something I would like it taken out. [11]*

Providers continue to embrace confidentiality to foster an environment in which patients will disclose information related to their health. However, in the realm of health information, the needs of those delivering, regulating, and paying for health care may be at odds with the principles of privacy and confidentiality [12,13]. Technological acquisition, storage, access to, and distribution of patient health data exacerbates that tension.

In addition to maintaining confidentiality, providers are subject to legal and ethical obligations to evaluate and document the encounter. Providers engage in narrative with the patient and form opinions throughout and across interviews [14]. Therefore it follows that the available EHR vocabulary must accommodate symptoms and modifiers in addition to diagnoses and summary statements [14]. Data entry systems must be seamless and unobtrusive, and should include handwriting or voice recognition in addition to standardized checklists and templates. Otherwise, provider time will be lost as physicians attempt to code findings during the encounter [14]. Since medical care itself is not standardized, it remains difficult to envision a "one size fits all" approach to medical record computing [8,15].

Although there has been debate among providers about the feasibility and safety of having all patient information computerized and available across institutions, the authors accept the premise that EHR implementation is inevitable because of the support for the idea from health care regulators, third-party payers, hospital administrators, and physician advocacy groups such as the American Medical Association [16].

Progress and Models

As EHR models have struggled towards maturity, some key questions have arisen. Debatable issues include the following: whether the originating record should supply complete data or a summary; whether the data subsequently generated is episodic or longitudinal; and whether patients and providers will either control which information is "pushed" to the central record or be spectators as comprehensive data is "pulled" by remote systems. The EHR models that are developing in Australia and the United States suggest some divergent answers to these questions. Although less visible than institutional (provider or governmental) models, a third EHR model focuses on a web-based, distributed "personal" longitudinal record. This model raises discrete quality and confidentiality issues.

Australia

Australia's proposed national health information network is called Health*Connect* [17]. The basic Health*Connect* model is to extract a summary record from locally collected patient data which is then aggregated to create a centralized Health*Connect* record that may then be shared among participating and authorized providers [18].

A Health*Connect* "event summary" consists of the "critical information considered to be useful to other health care providers involved in the future care of the consumer." [19] Thus, Health*Connect* does not create a comprehensive longitudinal record. Rather, patients, with their providers, will choose which elements may be extracted from an existing health

record and transmitted to the Health*Connect* record. Providers, with the consent of their patients, may subsequently add data to the Health*Connect* record. It follows, therefore, that *HealthConnect* is a "push" system, selectively sending data to a centralized record [20].

The patient controls which elements of the centralized record may be used for which purposes or displayed in which "views" [21]. For example, a patient might elect to include details of his psychotropic prescriptions in an event summary and consent to all his prescribing doctors viewing that data, but only consent to other mental health professionals viewing his psychiatrist's discharge order. The system's dedication to voluntary participation is desirable based on demonstrated patient interest in confidentiality. However, the summary data that is centralized may not fully support the system's secondary goals of disseminating professional education, supporting research, furthering utilization, increasing access, and improving quality [20]. Health*Connect* has completed 2 years of pilot testing. It is estimated that the system will save AUD $300 million per year by reducing errors and duplication of effort [20].

United States

The IOM has been critical of the rate of technology adoption by US hospitals [22]. Notwithstanding, and representing the public sector, the Department of Veterans Affairs is committed to process reform and technologically mediated delivery of services [23]. More broadly, the Consolidated Health Informatics (CHI) initiative is accelerating the use of common clinical vocabularies and messaging standards across federal agencies that process health data [24]. In addition to projects of national scope, some state governments have EHR launch initiatives; for example, Massachusetts has recently announced a statewide initiative, partially funded by the health insurer Blue Cross Blue Shield, with the goal of having a statewide electronic records system in place within five years [25]. Similar initiatives are being undertaken by some of the largest private providers; for example, Kaiser Permanente, the largest nonprofit health management organization (HMO) in the United States, with some 8.4 million members in 9 states and 12000 participating physicians, has recently adopted a 3-year, $1.8 billion electronic records program [26].Providing additional direction in developing EHR models have been the Connecting for Health initiative funded by the Markle Foundation [27], and the work of the EHR Collaborative [28], which consists of the major professional stakeholders such as the American Medical Association, and the Healthcare Information and Management Systems Society.

In the United States, as is the case in Australia and the UK [29], the purer EHR model is evolving at the national level. To date, the IOM [30] and the National Committee on Vital and Health Statistics (NCVHS) [31,32] have focused primarily on the *technical* aspects of EHR implementation in the United States. Both have identified two core components in the project: first, building a national health information infrastructure and, second, establishing data interoperability and comparability for patient safety data. In order to achieve data interoperability and comparability, NCVHS and IOM have recommended the adoption of core standardized EHR terminologies (eg, ICD-9 for diseases or symptoms [33], CPT-4 to code medical procedures, and services [34], and RxNorm for drug names and doses [35]). Considerable development is also underway to standardize event taxonomy (eg, adverse event or near-miss reporting using the College of American Pathologists' SNOMED CT taxonomy [36]) and to express knowledge representation such as clinical practice guidelines.

At this stage in the development of the US national model, its architects are concentrating on the interoperability and comparability of *all* patient safety-related data [37], designing a full "pull" architecture such that centralized and local records can import semantically similar data. Currently it is unclear which data consumers will choose to extract from remote systems or what limitations will be imposed, or by whom.

The Internet Alternative—the Personal EHR

Most EHR initiatives are national in scope and frequently government initiated or funded. EMR initiatives are typically hospital- or system-wide, yet are being designed with an eye to broader push or pull systems that will make wide-area use of such institutional data. A personal EHR model is quite different in concept. It assumes that individual patients will aggregate their diverse records and then make them selectively available to new or emergency providers. There are several subscription, web-based personal EHR systems such as PersonalMD.com [38] and Vital Vault [39] that provide secure web space in which patients can aggregate their medical data. Some of these systems also offer automated updating from select providers. Thus, the emerging model emulates popular personal finance applications (such as Microsoft Money or Intuit's Quicken) that allow for both end-user input and importation of data from institutional records to allow management of accounts. As with many emerging Internet-based health-related services, personal EHRs are immature, tend to exhibit limited functionality, and lack permanence [40,41].

Challenges

While Australia's Health*Connect* respects patient and provider choices and generates only limited data sets, the US system seems to be moving towards interoperability and comparability of *all* patient data, maximizing patient data flow into local and national systems but, arguably, at the cost of patient autonomy. The Australian system may pay too much attention to patient consent and jeopardize broader outcomes and reporting goals. Both institutional systems require careful scrutiny with regard to their costs, confidentiality, and liability risks. The nascent Personal EHR model generates additional concerns, which are similar to those experienced with other web-based products such as medical advice sites.

Cost

Considerable uncertainty exists regarding the costs associated with electronically mediated health initiatives and their allocation [42]. During transitional periods, costs rise as both traditional and technologically mediated models work in parallel. Most immediately, the health care industry will have to adjust to costs associated with evolving technologies and short system-lives. There has been recent controversy in the United

States over Congressional rejection of President Bush's initiative to expand funding for the Office for National Health Information Technology coordination (ONCHIT) of the Department of Health and Human Services; this will likely jeopardize public-sector EHR demonstration projects that were to have been funded out of that office [43].

Equally, there are practical, economic, political, and professional barriers that impede the acceptance of electronic records systems. Individual physicians or small practice groups have particular concerns about the costs and learning curves associated with electronic records systems [44]. Additionally, there are questions about whether to convert records retrospectively or whether electronic records systems should be prospective. Predictably, the medical community is concerned about costly dependence on proprietary technology companies, which could potentially monopolize the hardware and software required for interoperability. One possible solution would be for the mechanism of implementation of the EHR to be a public service built to public standards and/or under patient control [45].

Privacy and Confidentiality

An EHR system must satisfy its users regarding privacy, confidentiality, and security [46]. In the United States, the Health Insurance Portability and Accountability Act (HIPAA), passed in 1996 [47], committed the federal government to a process of "Administrative Simplification" to reduce health care costs. That mandate included regulatory authority to promulgate national Standards for Privacy of Individually Identifiable Health Information (PIHI) [48]. The PIHI regulations only regulate the disclosure of health data; they place no limitations on its the collection. Although the regulations limit use and disclosure with a "minimum necessary" rule [49], that limitation is inapplicable in cases of treatment or when disclosure is required by law [50]. Further, PIHI permits disclosure to a very broad range of public health, law enforcement, and judicial authorities [51], and provides for less than robust control of disclosures for secondary uses, such as marketing by providers [52]. Confusingly the PIHI regulations only supplement more rigorous state privacy laws. More recently, the HIPAA legislation has given rise to comprehensive federal security rules that govern health care transactions [53].Their limitations, notwithstanding the regulations made under HIPAA, apply to existing health records kept by most providers and are equally applicable to forthcoming EMR and EHR data. It appears unlikely, however, that US EHR developments will be accompanied by any additional protections, either by providing enhanced collection (privacy) or disclosure (confidentiality) rules or by derogating from a pure "pull" model of data aggregation.

Australian state [54] and federal (Commonwealth) governments aggressively protect patient information [55]. The Commonwealth National Privacy Principles [56] are broadly sensitive to the needs of the health information domain and protect patients with collection-centric (by placing limits on collection and granting consumers anonymity rights) and disclosure-centric rules as well as addressing data quality, data security, and access rights. In 2001, the Australian Federal Privacy Commissioner issued his nonbinding but influential initial Guidelines on Privacy in the Private Health Sector [57] that map the National Privacy Principles to the health context and provide for a robust collection-centric approach. In most cases, consent is required prior to collecting patient health information. This consent should include disclosure of the purposes for which the information is being collected. Further, the "[i]nformation collected should be limited to what is necessary for the health service provider's functions and activities." [58] The Guidelines state that a provider should "only use or disclose personal information for the primary purpose for which it was collected, or for directly related secondary purposes if these fall within the reasonable expectations of the individual" [59]. As a result, the Guidelines provide a satisfactory framework for emerging EHR models, while the Health*Connect* patient-controlled "push" model is intrinsically protective of patient interests.

The US PIHI rules regulating the disclosure of health data have less certain application outside traditional bricks-and-mortar providers, such as those engaged in Internet prescribing and web-based medical advice [60]. As a result, considerable attention needs to be paid to the confidentiality and security of data stored by Personal EHR businesses. In many cases the patient's protection will be limited to that granted by a privacy policy published by the personal EHR provider.

Litigation Risks

Privacy and confidentiality aside, providers already face legal costs with regard to their records. For example, a US provider's failure to maintain timely, legible, accurate and complete records will likely breach state licensure standards [61,62], with severe disciplinary implications [63,64], and may also jeopardize Medicare participation [65]. Improper record keeping may also give rise to medical malpractice liability [66]. In this context, at least one US court has expressed doubt as to the adequacy of a summary rather than comprehensive record [67].

EHR systems inevitably will contribute other costs for users because of interactions with the legal system. Emerging EHR systems, particularly those linked to CDSSs, will be vulnerable to actions focusing on design or other operational flaws [68]. Providers who adopt immature systems may face liability risks because of system deficiencies or insufficient training; those who wait for mature systems are likely to face actions for their failure to implement new but plaintiff-labeled "state-of-the-art" records and CDSSs [69]. Adoption of electronic records systems may also create more indirect legal costs. Litigants may attempt to leverage the new systems to promote their recovery in clinical negligence cases. For example, plaintiffs' attorneys may attempt to use data-mining tools to identify related occurrences to bolster evidence or use their clients' rights of access and modification to manipulate the patient record [70].

Conclusion

On April 26, 2004, President Bush announced the goal of assuring that most Americans have EHRs within the next 10 years [71]. To this end, the President appointed a National Health Information Technology Coordinator to guide the

"nationwide implementation of interoperable health information technology." [72]

If properly funded and nationally implemented, the US EHR model has the following potentials: to interconnect with and enhance other error-reducing and cost-saving technologies such as decision support systems; to streamline health care dataflow using an interoperable and standardized nomenclature; to improve quality by encouraging accurate and legible communication among providers; to automate adverse event and medical error disclosure; and to facilitate reliable and reproducible outcomes research and reporting [73].

As EHR progress continues, several important questions remain unanswered. Which is the preferable EHR model—a shared summary system or a full interpretational longitudinal record? How much say will or should patients and providers have regarding which health information is shared across systems? Would an interactive EHR increase patient interest and involvement in their own care? And, of course, will electronic records conquer the technical problems they pose, avoid the security and privacy costs their critics identify, and deliver lower costs and higher quality; or will they be responsible for still more costs and errors, while promoting the continued industrialization of health care delivery and subordinating patient autonomy and professional ideals to soulless systems?

It has never been more important for providers to be aware of emerging technology, to comprehend the tension between improved care and the preservation of patient privacy and autonomy, and to offer feedback to the American Medical Association and other professional bodies as these entities move to influence the development of the EHR.

Conflicts of Interest

None disclosed.

References

1. ; Institute of Medicine. Crossing the Quality Chasm: A New Health System for the 21st Century. Washington, DC: National Academies Press; Jun 1, 2001:15 URL: http://books.nap.edu/books/0309072808/html/index.html
2. ; Institute of Medicine. Crossing the Quality Chasm: A New Health System for the 21st Century. Washington, DC: National Academies Press; Jun 1, 2001:166 URL: http://books.nap.edu/books/0309072808/html/index.html
3. Hippisley-cox J, Pringle M, Cater R, Wynn A, Hammersley V, Coupland C, et al. The electronic patient record in primary care - regression or progression? A cross sectional study. BMJ 2003 Jun 28;326(7404):1439-1443 [FREE Full text] [PMC: 12829558] [doi: 10.1136/bmj.326.7404.1439] [Medline: 22712601]
4. . In: Aspden P, Corrigan JM, Wolcott J, Erickson SM, editors; Committee on Data Standards for Patient Safety, Board on Health Care Services, Institute of Medicine. Patient Safety: Achieving a New Standard for Care. Washington, DC: The National Academies Press; 2004:4 URL: http://www.nap.edu/catalog/10863.html
5. Kaushal R, Bates DW. Computerized Physician Order Entry (CPOE) with Clinical Decision Support Systems (CDSSs). In: Shojania KG, Duncan BW, McDonald KM, Wachter RM, editors. Making Health Care Safer: A Critical Analysis of Patient Safety Practices. Evidence Report/Technology Assessment, No. 43, Chap 6. AHRQ Publication No - 01-E058 (Prepared by the University of California at San Francisco - Stanford University Evidence-based Practice Centre). Rockville, MD: Agency for Healthcare Research and Quality; 2001. URL: http://www.ahrq.gov/clinic/ptsafety/ [accessed 2004 Dec 16]
6. Tang PC, Hammond WE. A Progress Report on Computer-Based Patient Records in the United States. In: Dick RS, Steen EB, Detmer DE, editors; Committee on Improving the Patient Record, Institute of Medicine. The Computer-Based Patient Record: An Essential Technology for Health Care. Rev ed. Washington, DC: National Academies Press; 1997. URL: http://books.nap.edu/html/computer/commentary.html [accessed 2004 Dec 16]
7. Tsai CC, Starren J. Patient participation in electronic medical records. JAMA 2001 Apr 4;285(13):1765. [Medline: 21176198] [doi: 10.1001/jama.285.13.1765]
8. Rashbass J. msJAMA. The patient-owned, population-based electronic medical record: a revolutionary resource for clinical medicine. JAMA 2001 Apr 4;285(13):1769. [Medline: 21176203] [doi: 10.1001/jama.285.13.1769-a]
9. Landro L. The informed patient: consumers need health-care data. In: Wall Street Journal Jan 29, 2004:D3.
10. Willison DJ, Keshavjee K, Nair K, Goldsmith C, Holbrook AM; Computerization of Medical Practices for the Enhancement of Therapeutic Effectiveness investigators. Patients' consent preferences for research uses of information in electronic medical records: interview and survey data. BMJ 2003 Feb 15;326(7385):373 [FREE Full text] [PMC: 12586673] [Medline: 22473881] [doi: 10.1136/bmj.326.7385.373]
11. Macdonald R. Commentary: A patient's viewpoint. BMJ 2001;322(7281):287 [FREE Full text] [doi: 10.1136/bmj.322.7281.287]
12. Mandl KD, Szolovits P, Kohane IS. Public standards and patients' control: how to keep electronic medical records accessible but private. BMJ 2001 Feb 3;322(7281):283-287 [FREE Full text] [Medline: 21096638] [doi: 10.1136/bmj.322.7281.283]
13. Markwell D. Commentary: Open approaches to electronic patient records. BMJ 2001;322:286 [FREE Full text]
14. Walsh SH. The clinician's perspective on electronic health records and how they can affect patient care. BMJ 2004 May 15;328(7449):1184-1187 [FREE Full text] [Medline: 15142929] [doi: 10.1136/bmj.328.7449.1184]

15. Safran C. msJAMA. Electronic medical records: a decade of experience. JAMA 2001 Apr 4;285(13):1766. [Medline: 21176199] [doi: 10.1001/jama.285.13.1766]
16. AMA throws support behind health IT coordinator. Modern Physician 2004 Dec 9.
17. ; Australian Government Department of Health and Ageing. HealthConnect. 2004 Nov 11. URL: http://www.healthconnect.gov.au/ [accessed 2004 Dec 16]
18. ; Australian Government Department of Health and Ageing. HealthConnect - an overiew. 2004 May. URL: http://www.healthconnect.gov.au/pdf/HealthConnect_overview_May2004.pdf [accessed 2004 Dec 16]
19. ; Australian Government Department of Health and Ageing. HealthConnect Business Architecture version 1.0. 2003 Apr. p. 20, sect 4.3 URL: http://www.healthconnect.gov.au/pdf/bav1.pdf [accessed 2004 Dec 17]
20. ; Australian Government Department of Health and Ageing. HealthConnect Business Architecture version 1.0. 2003 Apr. p. 30-31 URL: http://www.healthconnect.gov.au/pdf/bav1.pdf [accessed 2004 Dec 17]
21. ; Australian Government Department of Health and Ageing. HealthConnect Business Architecture version 1.0. 2003 Apr. p. 23, sect 4.5 URL: http://www.healthconnect.gov.au/pdf/bav1.pdf [accessed 2004 Dec 17]
22. . In: Aspden P, Corrigan JM, Wolcott J, Erickson SM, editors; Committee on Data Standards for Patient Safety, Board on Health Care Services, Institute of Medicine. Patient Safety: Achieving a New Standard for Care. Washington, DC: National Academies Press; May 10, 2004:436 URL: http://www.nap.edu/catalog/10863.html
23. ; VA National Center for Patient Safety (NCPS). Creating a Culture of Safety. URL: http://www.patientsafety.gov/vision.html [accessed 2004 Dec 16]
24. ; Consolidated Health Informatics. Home page. URL: http://www.whitehouse.gov/omb/egov/gtob/health_informatics.htm [accessed 2004 Dec 16]
25. Peter J. Mass. launches computerized medical files. Washington Post/Associated Press. 2004 Dec 6. URL: http://www.washingtonpost.com/wp-dyn/articles/A41136-2004Dec6.html [accessed 2004 Dec 16]
26. Rundle RL. Big HMO plans to put medical records online. In: Wall Street Journal Feb 4, 2003:D4.
27. ; Markle Foundation, Data Standards Working Group. Connecting for Health - A Public-Private Collaborative, Report and Recommendations. 2003 Jun 5. URL: http://www.connectingforhealth.org/resources/dswg_report_6.5.03.pdf [accessed 2004 Dec 16]
28. ; EHR Collaborative. Home page. URL: http://www.ehrcollaborative.org/ [accessed 2004 Dec 16]
29. ; National Health Service, United Kingdom. National Programme for IT in the NHS. URL: http://www.npfit.nhs.uk/ [accessed 2004 Dec 16]
30. . In: Aspden P, Corrigan JM, Wolcott J, Erickson SM, editors; Committee on Data Standards for Patient Safety, Board on Health Care Services, Institute of Medicine. Patient Safety: Achieving a New Standard for Care. Washington, DC: National Academies Press; May 10, 2004:1-28 URL: http://www.nap.edu/catalog/10863.html
31. ; National Committee on Vital and Health Statistics. Report to the Secretary of the US Department of Health and Human Services on Uniform Data Standards for Patient Medical Record Information. 2000 Jul 6. URL: http://www.ncvhs.hhs.gov/hipaa000706.pdf [accessed 2004 Dec 16]
32. ; National Committee on Vital and Health Statistics. Recommendations for PMRI terminology standards. 2003 Nov 5. URL: http://www.ncvhs.hhs.gov/031105lt3.pdf [accessed 2004 Dec 16]
33. ; National Center for Health Statistics, Centers for Disease Control and Prevention. International Classification of Diseases, Ninth Revision, Clinical Modification (ICD-9-CM). URL: http://www.cdc.gov/nchs/about/otheract/icd9/abticd9.htm [accessed 2004 Dec 16]
34. ; American Medical Association. CPT Process - How a Code Becomes a Code. 2004 Nov 4. URL: http://www.ama-assn.org/ama/pub/category/3882.html [accessed 2004 Dec 16]
35. ; National Library of Medicine. Unified Medical Language System, RxNorm. 2004 Nov 2. URL: http://www.nlm.nih.gov/research/umls/rxnorm_main.html [accessed 2004 Dec 16]
36. ; SNOWMED International. SNOMED CT. URL: http://www.snomed.org/snomedct/index.html [accessed 2004 Dec 16]
37. . In: Aspden P, Corrigan JM, Wolcott J, Erickson SM, editors; Committee on Data Standards for Patient Safety, Board on Health Care Services, Institute of Medicine. Patient Safety: Achieving a New Standard for Care. Washington, DC: National Academies Press; May 10, 2004:438 URL: http://www.nap.edu/catalog/10863.html
38. ; PersonalMD. Home page. URL: http://www.personalmd.com/ [accessed 2004 Dec 16]
39. ; VIMSystems. Vital Vault. URL: http://www.vimsystems.com/prod_vault.htm [accessed 2002 Dec 16]
40. Schneider JH. Online personal medical records: are they reliable for acute/critical care? Crit Care Med 2001 Aug;29(8 Suppl):N196-N201. [Medline: 21387190] [doi: 10.1097/00003246-200108001-00009]
41. Kim MI, Johnson KB. Personal health records: evaluation of functionality and utility. J Am Med Inform Assoc 2002;9(2):171-180. [PMC: 11861632] [Medline: 21850602] [doi: 10.1197/jamia.M0978]
42. Hawryluk M. Push continues for electronic health records. Bills set the foundation for action in the next Congress. American Medical News. 2004 Jun 14. URL: http://www.ama-assn.org/amednews/2004/06/14/gvsc0614.htm [accessed 2004 Dec 16]
43. Lohr S. Health Care Technology Is a Promise Unfinanced. New York Times. 2004 Dec 3 p. C5.
44. Richmond R. Small Business: Doctors See Healthy Returns in Digital Records. Wall Street Journal 2004 Dec 7:B1.

45. Mandl KD, Szolovits P, Kohane IS. Public standards and patients' control: how to keep electronic medical records accessible but private. BMJ 2001 Feb 3;322(7281):283-287 [FREE Full text] [Medline: 21096638] [doi: 10.1136/bmj.322.7281.283]
46. Terry NP. Privacy and the health information domain: properties, models and unintended results. Eur J Health Law 2003 Sep;10(3):223-237. [Medline: 23094590] [doi: 10.1163/157180903770847517]
47. Health Insurance Portability and Accountability Act of 1996 (HIPAA). (Pub.L. 104-191, Aug. 21, 1996, 110 Stat. 1936).
48. Standards for Privacy of Individually Identifiable Health Information (PIHI), Federal Register. (codified at 45 CFR §160, §164).
49. 45 CFR. §164.502(b)(1).
50. 45 CFR. §164.502(b)(2).
51. 45 CFR. §164.512.
52. 45 CFR. §164.508.
53. Health Insurance Reform: Security Standards, 68 Federal Register 8334. 2003. (codified at 45 CFR §160, §162, §164) URL: http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/03-3877.htm [accessed 2004 Dec 16]
54. ; Office of the Health Services Commissioner, Commonwealth of Australia. Victorian Health Privacy Principles extracted from the Health Records Act. 2001. URL: http://www.health.vic.gov.au/hsc/hppextract.pdf [accessed 2004 Dec 16]
55. ; Office of the Federal Privacy Commissioner, Commonwealth of Australia. The Commonwealth Privacy Amendment (Private Sector) Act 2000 extended the operation of the Privacy Act of 1988 to cover the private sector, including healthcare. Effective from December 21, 2001 URL: http://www.privacy.gov.au/act/privacyact/index.html [accessed 2004 Dec 16]
56. ; Office of the Federal Privacy Commissioner, Commonwealth of Australia. National Privacy Principles (Extracted from the Privacy Amendment (Private Sector) Act. 2000. URL: http://www.privacy.gov.au/publications/npps01.html [accessed 2004 Dec 16]
57. ; Office of the Federal Privacy Commissioner, Commonwealth of Australia. Guidelines on Privacy in the Private Health Sector. 2001 Nov 9. URL: http://www.privacy.gov.au/publications/hg_01.html [accessed 2004 Dec 17]
58. ; Office of the Federal Privacy Commissioner, Commonwealth of Australia. Guidelines on Privacy in the Private Health Sector (November 9, 2001). 2001 Nov 9. Sect 1.2: Collect only necessary information URL: http://www.privacy.gov.au/publications/hg_01.html [accessed 2004 Dec 17]
59. ; Office of the Federal Privacy Commissioner, Commonwealth of Australia. Guidelines on Privacy in the Private Health Sector (November 9, 2001). 2001 Nov 9. Sect 2: Use and disclosure URL: http://www.privacy.gov.au/publications/hg_01.html [accessed 2004 Dec 17]
60. Terry NP. Prescriptions sans frontières (or how I stopped worrying about Viagra on the Web but grew concerned about the future of healthcare delivery). Yale J Health Policy Law Ethics 2004;4(2):183-272. [Medline: 101785425]
61. NRS. §630.3062(1) (Nevada).
62. Wyo. Stat. §33-26-402 (Wyoming).
63. Schwarz v. Board of Regents, 89 AD2d 711, 453 NYS2d 836. (NY App Div 3d Dep't 1982).
64. Nieves v. Chassin, 214 AD2d 843, 625 NYS2d 344. (NY App Div 3d Dep't 1995).
65. 42 CFR. §482.24(b)-(c).
66. Brown v. Hamid, 856 SW2d 51. (MO 1993).
67. Thomas v. United States, 660 F Supp 216, 218. (DDC 1987).
68. Fernando B, Savelyich BSP, Avery AJ, Sheikh A, Bainbridge M, Horsfield P, et al. Prescribing safety features of general practice computer systems: evaluation using simulated test cases. BMJ 2004 May 15;328(7449):1171-1172 [FREE Full text] [Medline: 15142922] [PMC: 15142922] [doi: 10.1136/bmj.328.7449.1171]
69. Terry NP. When the “machine that goes ‘ping’” causes harm: default torts rules and technologically-mediated health care injuries. St Louis Univ Law J 2002;46:37-59.
70. Terry NP. An eHealth diptych: the impact of privacy regulation on medical error and malpractice litigation. Am J Law Med 2001;27(4):361-419. [Medline: 21825759]
71. ; The White House. Transforming Health Care: The President's Health Information Technology Plan. URL: http://www.whitehouse.gov/infocus/technology/economic_policy200404/chap3.html [accessed 2004 Dec 16]
72. Executive Order 13335 of April 27, 2004, Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator, 69 Federal Register 24059, Sect. 3. 2004 Apr 30. URL: http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2004/pdf/04-10024.pdf [accessed 2004 Dec 16]
73. ; Australian Council for Safety and Quality in Health Care. Open Disclosure Standard: A National Standard for Open Communication in Public and Private Hospitals, Following an Adverse Event in Health Care. 2003 Jul. URL: http://www.safetyandquality.org/articles/publications/OpenDisclosure_web.pdf [accessed 2004 Dec 16]

Abbreviations

CDSS: computerized decision support system

CHI: Consolidated Health Informatics
CPOE: computerized physician order entry
EHR: electronic health record
EMR: electronic medical record
HIPAA: Health Insurance Portability and Accountability Act
HMO: health management organization
IOM: Institute of Medicine
IT: information technology
NCVHS: National Committee on Vital and Health Statistics
PIHI: Standards for Privacy of Individually Identifiable Health Information
RFID: Radio Frequency Identification

submitted 17.02.05; peer-reviewed by J Powell; accepted 25.02.05; published 14.03.05

Please cite as:
Gunter TD, Terry NP
The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions
J Med Internet Res 2005;7(1):e3
URL: http://www.jmir.org/2005/1/e3/
doi: 10.2196/jmir.7.1.e3
PMID: 15829475