Use of Digital Health Records Raises Ethics Concerns

Beverly Kopala, PhD, RN • Mary Ellen Mitchell, MA, RN

ABSTRACT

There has been a proliferation in the use of digital health records. Although electronic records have many benefits, concerns have been raised about associated risks and barriers. This article focuses on risks associated with development, utilization, and maintenance of provider-owned electronic medical records and institution-owned electronic health records. Strategies to reduce risks and overcome barriers are also offered. Attention to these issues can minimize risks and improve healthcare services delivered to consumers.

Even if it has not yet done so, the digital health record will eventually touch everyone's life, on a personal and/or a professional level. The digital age has propelled us into areas and provided opportunities that, not long ago, were never even imagined. Spurred by the American Recovery and Reinvestment Act of 2009, the full potential of electronic health records (EHRs) is just beginning to be felt in the United States.

Fulfilling a federal government goal to establish a nationwide health network of interoperable EHRs by 2014 involves transitioning providers and hospitals to EHR use and developing the infrastructure to support the safe, secure, and accurate exchange of data.[1] Fully interoperable EHRs have the potential to allow data from multiple sources, internal and external to the health system, to enter a patient's record.[2] Depending on its design, data have the potential to flow from the patient's EHR to various other sources. Although not yet widely supported, system design may allow physicians to have access to the personal health record (PHR) of patients who are maintaining their own health record in an accessible system.[2] Users of provider-controlled electronic medical records (EMRs) and institution-owned EHRs, whether fully interoperable or not, need to develop policies and procedures

Author Affiliations: Niehoff School of Nursing, Loyola University Chicago (Dr Kopala); Care Management/Social Services, QI, NorthShore University Health System, Evanston (Ms Mitchell), Illinois.

The authors have disclosed that they have no significant relationships with, or financial interest in, any commercial companies pertaining to this article.

Correspondence: Beverly Kopala, PhD, RN, 1032 W Sheridan Rd, Granada Center, Room 360, Chicago, IL 60660 (bkopala@luc.edu).

DOI: 10.1097/NHL.0b013e31822aafbd

that consider state and federal laws, professional standards, and accrediting bodies such as The Joint Commission, Healthcare Facilities Accreditation Program, and Det Norske Veritas (DNV) when implementing this technology.

The activities of regional health information organizations and regional health improvement collaboratives support achievement of this goal. Regional health information organizations and regional health improvement collaboratives are multistakeholder organizations composed of healthcare provider facilities, public health departments, payers, and others. They are designed to facilitate information technology (IT) adoption and implementation of EHRs by providers and to advance electronic health information exchange across organizations and between various healthcare information systems within a geographic area.[3,4]

Multiple benefits are expected to accrue from this nationwide initiative. Anticipated benefits include improvement in quality and continuity of care by decreasing medical errors, reducing health disparities, improving the health of the public, and advancing education and research.[1] The inevitability of the transition to EHRs, anticipated cost savings, improved patient care/safety, incentive programs, and the ability to track quality indicators serve as drivers for their implementation.[5] Although the use of EMRs and EHRs offers many benefits, there are risks associated with the expansion, development, and maintenance of medical/health information in electronic form.

Risks and Risk Reduction Strategies

Various risks are linked to implementation of EMRs/EHRs. Whereas primary risks are associated with patient privacy and data security breaches, others are related to cost, system implementation, data inaccuracies, and related liability issues.[5–7] Barriers include resistance of healthcare professionals to this digital format.[6–9] Four risk categories with selected risk reduction strategies are discussed in the following sections. Some related liability issues are integrated into the discussion of each category.

Privacy and Security Breaches

The patient or legal representative has responsibility for the care, custody, and control of the health record[10] whether on paper or in electronic format. Adult patients are expected to make decisions about their healthcare, including what medical information will be shared with healthcare providers. When a patient is unable to do so because of age, incompetence, or incapacity, decisions about information sharing should be made by the patient's legal representative/legal guardian and must be made in the patient's best interests. The legal representative of an incompetent adult patient is his/her legal guardian, the agent designated in an incapacitated patient's power of attorney for healthcare, the deceased patient's personal representative or spouse, or other adult member of the patient's immediate family if there is no surviving spouse.[10] States are recognizing the need to broaden a legal representative's access to the patient's record in some cases. For example, as of July 1, 2011, in the state of Illinois, the legal representative who has the patient's power of attorney for healthcare has full access to the patient's medical record regardless of the patient's mental capacity.[11,12]

Concerns specific to pediatric and adolescent patients, whose understanding and ability to consent to access vary with age and situation, have been voiced.[13] The Health Insurance Portability and Accountability Act protections for the pediatric population are complex because legal representatives can have long-term access to the record, and different users and contributors to the record have different user rights and contributor expectations.[13]

Healthcare institutions, insurance companies, and others will require access to these data if EHRs are to function as designed. Although multiple users (patients, select family members, providers, employers, third-party payers, and others) may benefit from the use of electronically stored medical information, shared access raises issues about privacy, confidentiality, and security. Factors contributing to the effectiveness, efficiency, and integration of EHRs and their networks simultaneously present the greatest privacy threats.[14]

Determining who can and should oversee, protect the record, and make decisions about release of a patient's healthcare information can be a struggle for healthcare providers and institutions. Respecting choices can require the involvement of clinicians, ethicists, and counsel.[13]

The public is aware of some potentially negative outcomes associated with data sharing, especially when data are shared with insurance companies. For example, insurance companies base reimbursement decisions on shared patient information. Once this information is released to insurance companies, concerns remain that private health information may be used as a basis for raising insurance rates or canceling coverage.

Security breaches threaten patient privacy when confidential health record information is made available to others without the individual's consent or authorization. When data are stored, ''secure'' files are vulnerable to being compromised, despite firewalls, encryption, and password protection, by the curious or by others who are intent on hacking into a data storage system to disrupt the flow of information, damage files, or obtain unauthorized access to information. Storing records in files that are not password protected, sharing passwords with unauthorized individuals, and leaving computers with sensitive information unattended, as well as storing data at multiple sites, such as on an original and backup server, increase opportunities for security breaches.

Unauthorized access to or release of health information affects not only the individual whose records have been breached—but has the potential to affect family members as well. For example, one's family history may reveal

genetic information about other family members, potentially making them vulnerable to discrimination, stigmatization, or receipt of potentially undesired information, such as a genetic susceptibility or possible inherited disease, especially if the disease has no cure or treatment.

There are some safeguards in place to protect patient privacy and enhance security. In order for their health information to be shared with third parties, patients or their legal representative must sign a waiver permitting release of this information. User access is also limited or monitored. In a role-based access privacy system, access to the digital record is limited and based on need to perform work functions. An alternative is open access, whereby access to the full EHR is available to all healthcare disciplines and healthcare workers regardless of role. Their record utilization is monitored by the chief privacy officer. Although state and federal laws, as well as organizational policies, address privacy protections, state laws and organizational policies vary greatly—some providing more protection than others.

In addition to the standard expectations of the Health Insurance Portability and Accountability Act confidentiality requirements, specific policies and procedures serve to maintain patient privacy and confidentiality. For example, employees must be expected to use their own ID to access patient digital records, always log off when leaving a terminal, and not share their ID with anyone so unauthorized access under another's ID cannot occur. These same types of requirements apply to students who need short-term access to patient records to provide and document care.

To ensure compliance with hospital policy, routine random audits should be conducted. When potentially inappropriate access to a medical record is identified, the system can yield information about the name of the individual gaining access; the time, date, and screens accessed; and the duration of the review. This information is useful when determining whether the access is the result of an error or an intentional, unauthorized chart review. The employee's and/or physician's role in the organization as well as patient assignments can be evaluated in order to determine appropriateness of record access. Patients should be informed that they may request a log of everyone who has had access to their record, and these requests must be honored with an audit. Sanctions for breaches in protocol, such as staff members leaving a terminal unattended without logging off and/or employees gaining inappropriate access to patient information, should be imposed. These sanctions should include disciplinary action up to and including termination of involved individuals.

Corporate medical groups and independent physicians given key fob linkage to digital records can have patient medical information access and can participate in care from afar—even from abroad in emergencies. The patient has the advantage of having a physician with knowledge of their history and baseline status. Key fob access must be disabled once the provider leaves the system.

Outside vendors, both on-site and off-site, create special privacy issues. Employee-only access to the EMR requires any external vendor to access and navigate the record on-site under the authorization and oversight of an employee. When off-site access to the record is required, a telefax report can be designed to limit the content and recipients of all released data. This process can also control errors inherent in paper faxing. External consultants given access should meet hospital-specific requirements such as providing the social security number or other individual identifier of each user before contractual agreements are finalized.

Given that legal action against the facility can be an outcome of privacy and confidentiality violations, diligence must be maintained. Electronic audit and oversight could not be implemented with paper records because documentation of access to the medical record was not able to be tracked.

Cost

The process of developing, implementing, and maintaining EHRs requires adequate funds and the involvement of many individuals, including clinicians, information technologists, educators, and consultants.[15] Selection of a system and software capable of meeting the current and anticipated needs of the providers and healthcare system is critical to the cost investment and return on investment (ROI). Maintenance costs include ongoing system enhancements as well as innovations in the ''pipeline.''

The initial financial investment to convert to an electronic record format, even for a small hospital system, can range upward of tens of millions of dollars. Training, maintenance, and enhancements are additional millions. Estimated cost per healthcare provider practice implementing an EMR is $40,000 to $100,000, whereas capital outlay at the system level has been estimated at $40 million to $350 million.[5] There have been claims that a true business case for implementing EHRs, at least in ambulatory settings, is lacking, and their implementation has been held to a different standard than that required for traditional capital investment decisions.[5]

All costs, after the initial investment, can be expected to be transferred to the business costs of patient care. As reimbursements are declining, the variance in cost versus savings will have a greater or lesser impact based on the financial solidarity of the facility. With any of these systems, allocating funds to development and maintenance of a new system requires a new revenue stream or financial reallocation decisions. In the latter case, when funds are directed to installation and maintenance of a new system, fewer resources will be available for other system needs.

All of these considerations are essential to substantiate a viable business plan for any organization that is making this significant of an investment. The ROI should reflect savings, including malpractice insurance and malpractice claims for patient care errors, particularly as a result of the reduction in medication errors. Cost savings in conjunction with positive revenue gains from ''meaningful use'' are included in the ROI calculation.

If providers and hospitals can demonstrate meaningful use, government support can provide a new revenue

stream. As a result of the American Recovery and Reinvestment Act of 2009, the Department of Health and Human Services established Medicare and Medicaid Incentive Programs to financially motivate eligible physicians and hospitals to successfully demonstrate meaningful use of certified EHR technology by supporting the purchase and effective and efficient use of quality systems to capture data and share information electronically.[1] Meeting meaningful use criteria requires demonstration of compliance with established criteria designed to facilitate the move to EHRs in a stepwise fashion. In stage 1 of the program (years 2011 and 2012), eligibility for financial incentives is linked to successful adoption, implementation, and upgrade of EHRs or demonstration of meaningful use in the first and following participation years.[16,17] Demonstration of meaningful use includes measurement of positive clinical outcomes as a result of enhanced EMR/EHR functions.

System Implementation

With the selection of a health information management system come concerns related to the adequacy of the system. Hardware, software, and technical equipment must be able to satisfy user needs, goals, and expectations. The process of implementation of the system involves the expertise of the chief information officer and the entire IT staff along with personnel from all departments that provide operational oversight. Once the system is implemented, ongoing maintenance involves evaluation and installation of continuing upgrades to meet system expansion needs in both inpatient and outpatient settings.

When any 2 systems must be integrated, an interface is created. These interfaces among healthcare delivery systems are critical to the overall success of the implementation process and if the advantages of the electronic network are to be realized. Interface issues are the greatest system risk because these failures can be initially invisible until their impact is felt. Maintenance and testing of these interfaces on a routine basis are essential to controlling this major risk.

To minimize the risk of user errors, staff must be trained prior to system implementation and continue to receive ongoing support from clinicians with IT training and certification through testing. Information technology staff can educate, troubleshoot, and support end users throughout implementation and beyond. Paper chart backup should be in place for any system downtime and initially may be a part of a dual system Notification of downtime, planned and unplanned, must be communicated via e-mail and/or overhead announcements on the level of other color code announcements. System clear announcements must follow when systems go back up. System functions must be repeatedly assessed after go-live, and multiple adjustments should be expected.

Data Inaccuracies

Digital health records are seen as one mechanism to improve patient safety by reducing healthcare errors.[1] However, concerns have been raised about the quality or accuracy and reliability of data entered into the electronic record. Because the records are longitudinal by nature, they can contain extensive amounts of data that may not be current or useful to or needed by multiple care providers who can easily access the electronic record from various locations.[10] Incomplete data, inaccurate data entry by providers or by patients in the case of an interoperable PHR, improper use of optional functions such as ''cut and paste'' that may increase ease of use and efficiency for providers but may result in an inaccurate representation of the patient's current condition and treatment, and loss or destruction of data during data transfer raise concerns about the accuracy of the database upon which patient care decisions are based.[6] Both EMRs and EHRs can also be populated with inaccurate or incomplete data when data sharing among types of records or multiple systems has occurred or when fraudulent actions compromise the integrity of the information in the record.

The annual cost of healthcare fraud is conservatively estimated to be about 3%, or about 68 billion of healthcare dollars spent, but estimates range as high as 10%.[18] Fraudulent acts that have been perpetrated by a small number of healthcare professionals include falsifying diagnoses and/or exaggerating the severity of a patient's condition and billing for services not provided. Non-healthcare professionals have also attempted and/or successfully engaged in large-scale fraud, such as billing Medicare, Medicaid, and private insurance companies for patient services not provided or required.

Fraud has become so pervasive that federal and state governments have enacted legislation to strengthen fraud detection, management, and reporting. For example, those submitting reimbursement claims to Medicare and Medicaid are required to exercise due diligence in proactively identifying and preventing fraud given that lack of knowledge or unintentional deception or misrepresentation is not acceptable.[11]

Medical identity theft, a growing problem, also results in the input of inaccurate information into the record of the victim. Not only may a person's insurance company be billed for medical services not provided to the actual policy holder, but also, even more concerning, the patient's future treatment may be guided by misinformation that neither the patient nor provider immediately recognizes.[19] The risk of medical identity theft is reduced when patients are required to present a picture ID when seeking healthcare services.

When information in the digital record conflicts, the data need to be reconciled in order to decrease the chance that decisions are impaired by inaccurate information. Correcting erroneous or inaccurate information can be difficult because that misinformation may already have been shared with others, including providers and insurers, by the time the error has been recognized.

The skill base of the EHR user directly correlates with the quality of documentation, and ensuring adequate skill level is the major operational issue. Ongoing commitment to the skill level of the EHR user is critical to the overall accuracy of the record. The initial investment in the system is dominated by training of staff prior to and on a

continuum once an organizational electronic system is live. For example, investment in pre–''go live'' and ''go-live and beyond'' education is most effective when trainers are on-site 24/7. The EHR is a powerful tool when in the hands of an electronically trained clinician, but, if that investment has not been made, the full capacity of the electronic tool is diminished, accuracy and quality of the content are suboptimal, and patient care could be negatively affected. In advance of a new go-live, the system may ''freeze'' for any additional changes so all staff can be adequately prepared for the new implementation changes in the system.

In addition to the inherent benefits/risks of EMRs/EHRs, there are additional challenges with organizational and personnel barriers. Some of these barriers, and selected strategies to ameliorate them, are identified in the following sections.

Addressing Barriers to EMR/EHR Implementation

Healthcare providers have demonstrated some resistance to implementation of EHRs in addition to time and financial constraints.[9] These changes can threaten physicians' and nurses' deeply engrained culture of values and beliefs about control of information and challenge traditional lines of authority and organizational power structures.[9] A review of the literature between 2000 and 2007 revealed nurses' negative perceptions of the EHR.[8] The literature supported (1) a lack of attention to the flow of nursing work, (2) inability to capture the invisible or intangible work that nurses do, (3) increased workload due to problems associated with system barriers, (4) inadequate training, (5) lack of useful outcome data to improve patient care, and (6) limited involvement of clinicians in selecting, implementing, and maintaining the system.[8]

Some physicians have indicated reluctance to adopt EMRs because of concerns about additional unreimbursed work.[20] Rather than convert ''old'' patient records to electronic format, some providers have made the conversion with the patient's first office visit following EMR implementation. When digital records are networked, conflicting rights of ownership also serve as a disincentive to their use.[21] Inconsistencies and duplications in incentive programs designed to spur use of IT by physicians also serve as limitations.[22]

The literature offers some strategies for addressing and overcoming barriers.[15,23–25] These include maintaining clear communication at all levels of the organization throughout the process, recognizing the effects of the organizational culture and capitalizing on strengths, maintaining realistic expectations, using effective change management strategies, and having a shared vision. Achieving user buy-in, providing quality adequate training that sufficiently prepares staff and fits staff needs, attending to workflow needs and patterns, having adequate and sufficient policies to guide implementation and maintenance of the system, ensuring awareness of those policies, and having a contingency plan for anticipated system downtime and other potential malfunctions are also suggested strategies.

Research and QI Initiatives

Although EHRs promise improved quality care, increased patient satisfaction, and lower costs, more research is needed to confirm these expectations. A review of 100 research articles published in the PHR literature between 1950 and 2007 revealed that the areas of function evaluation, adoption and attitudes, privacy and security, and architecture present significant opportunities for research.[20] In addition, health, medical, and clinical research, associated with implementing the American Recovery and Reinvestment Act of 2009, is significant to advancing the health of the nation.

Data in electronic records can also be used to support quality improvement initiatives that include measuring nursing care through nursing documentation.[26,27] Given the potential to access a wealth of information in digital medical/health information records, there is a need to weigh the patient's right to privacy against the potential public health and other benefits from use of aggregated, deidentified data for research.

Conclusion

Although EMRs offer many significant benefits, the future of healthcare demands that their risks be recognized and properly managed or overcome. Electronic medical record/EHR capacities must be maximized in order to enhance communication and improve the quality, safety, efficiency, and effectiveness of healthcare and healthcare delivery systems.

Multiple strategies are available to reduce risks and overcome barriers to the implementation of digital health records. Some general strategies that cross healthcare settings have been offered here. Users will find additional risks and strategies that are specific to the various settings in which healthcare services are offered. Leadership, teamwork, flexibility, and adaptability are keys to finding solutions that work.

REFERENCES

1. American Recovery and Reinvestment Act, HR 1, 111th Congress, 1st Session. 2009. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.pdf. Accessed June 14, 2011.
2. Francis LP. The physician-patient relationship and a national health information network. *J Law Med Ethics*. 2010;38(1):36–49.
3. Feinstein KW. Regional Health Improvement Collaboratives. Essential elements for successful healthcare reform. http://www.wchq.org/news/documents/03-16-11_Regional_Collaboratives.pdf. Published March 16, 2011. Accessed June 15, 2011.
4. US Department of Health and Human Services. Health Resources and Services Administration. What is a regional health information organization (RHIO)? http://www.hrsa.gov/healthit/toolbox/RuralHealthITtoolbox/Collaboration/whatisrhio.html. Accessed June 15, 2011.
5. Song PH, McAlearney AS, Robbins J, McCullough

JS. Exploring the business case for ambulatory electronic health record system adoption. *J Healthcare Manage* [serial online]. 2011;56(3):169–180. Ipswich, MA: Academic Search Premier. http://web.ebscohost.com/ehost/detail?sid=5ba93d45-b8a0-4072-a8d2-15ee2c834aa9%40sessionmgr11&vid=4&hid=18&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=aph&AN=60899445. Accessed June 19, 2011.

6. North Carolina Healthcare Information and Communications Alliance, Inc. The benefits and risks of electronic health records. http://www.nchica.org/GetInvolved/CACH/EHRbenefits-risks.htm. Accessed June 9, 2011.
7. Thakkar M, Davis DC. Risks, barriers and benefits of EHR systems: a comparative study based on size of hospital. *Perpect Health Inf Manag*. 2006;3(5). http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2047303/pdf/phim0003-0005.pdf. Accessed June 14, 2011.
8. Sassen EJ. Love, hate, or indifference: how nurses really feel about the electronic health record system. *Comput Inform Nurs*. 2009;27(5):281–287.
9. Thede L. Informatics: electronic records and organizational culture. *Online J Issues Nurs*. 2009;14(3). http://www.nursingworld.org/MainMenuCategories/ANAMarketplace/ANAPeriodicals/OJIN/Columns/Informatics/Electronic-Records-Organizational-Culture.aspx. Accessed July 21, 2011.
10. American Health Information Management Association. The legal process and electronic health records. http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_028134.hcsp?dDocName=bok1_028134?wtag=wtag647. Accessed June 18, 2011.
11. Illinois Hospital Association. IHA News & Memos. The Illinois statutory health care power of attorney. January 3, 2011. http://www.ihatoday.org/News-and-Reports/News-and-Memos/Content/The-Illinois-Statutory-Health-Care-Power-of-Attorney/39.aspx. Accessed June 18, 2011.
12. Ill 96th General Assembly SB 1877 (PA 96-1195). http://www.ilga.gov/legislation/BillStatus.asp?DocNum=1877&GAID=11&DocTypeID=SB&LegID=57995&SessionID=84&GA=97&SpecSess=0. Accessed June 18, 2011.
13. Bourgeois FC, Taylor PL, Emans SJ, Nigrin DJ, Mandl KD. Whose personal control? Creating private, personally controlled health records for pediatric and adolescent patients. *J Am Med Inform Assoc*. 2008;15(6):737–743.
14. Rothstein MA. The Hippocratic bargain and health information technology. *J LawMed Ethics*. 2010;38(1):7–13.
15. Bostrom AC, Schafer P, Dontje K, Pohl JM, Nagelkerk J, Cavanagh SJ. Electronic health record: implementation across the Michigan academic consortium. *Comput Inform Nurs*. 2006;24(1):44–52.
16. Hoffman S, Podgurski A. Meaningful use and certification of health information technology: what about safety. *J Law Med Ethics*. 2011:77–80.
17. US Department of Health and Human Services. Centers for Medicare & Medicaid. CMS EHR meaningful use overview. http://www.cms.gov/EHRIncentivePrograms/30_Meaningful_Use.asp. Accessed June 2, 2011.
18. National Health Care Anti-Fraud Association. Anti-Fraud Resource Center. The problem of health care fraud. Consumer alert: the impact of health care fraud on you. http://www.nhcaa.org/eweb/DynamicPage.aspx?webcode=anti_fraud_resource_centr&wpscode=TheProblemOfHCFraud. Accessed June 18, 2011.
19. Federal Trade Commission. Facts for consumers. Medical identity theft. http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt10.pdf. Published January 2010. Accessed June 20, 2011.
20. Kaelber DC, Jha AK, Johnston D, Middleton B, Bates DW. A research agenda for personal health records. *J Am Med Inform Assoc*. 2008;15(6):729–736.
21. Hall MA, Schulman KA. Ownership of medical information. *JAMA*. 2009;301(12):1282–1284.
22. Electronic health records [Capital Health Call]. *JAMA*. 2011;305(14):1402.
23. Lorenzi NM, Kouroubali A, Detmer DE, Bloomrosen M. How to successfully select and implement electronic records (EHR) in small ambulatory practice settings. *BMC Med Inform Decis Mak*. 2009;9(15). http://www.biomedcentral.com/1472-6947/9/15. Accessed July 21, 2011.
24. Valerius JD. The electronic health record: what every information manager should know. *Inf Manage J*. 2007;41(1):56–59. Ipswich, MA: Academic Search Premier. http://web.ebscohost.com/ehost/results?sid=c53a4ea4-deba-400d-971d-10ccde1eb202%40sessionmgr15&vid=2&hid=8&bquery=%28JN+%26quot%3bInformation+Management+Journal%26quot%3b+AND+DT+20070101%29&bdata=JmRiPWFwaCZ0eXBlPTEmc2l0ZT1laG9zdC1saXZl. Accessed June 19, 2011.
25. Yoon-Flannery KO, Zandieh SO, Kuperman GJ, Langsam DJ, Hyman D, Kaushal R. A qualitative analysis of an electronic health record (EHR) implementation in an academic ambulatory setting. *Inform Prim Care*. 2008;16(4):277–284. Ipswich, MA: Academic Search Premier. http://docserver.ingentaconnect.com/deliver/connect/rmp/14760320/v16n4/s5.pdf?expires=1311276124&id=63667029&titleid=6073&accname=Loyola+University+-+Chicago&checksum=FA325C874FA5BB6E3E51A0F5BEB797D8. Accessed June 19, 2011.
26. Burkhart L, Androwich I. Measuring spiritual care with informatics. *Adv Nurs Sci*. 2009;32(3):200–210.
27. Westra BL, Subramanian A, Hart CM, et al. Achieving "meaningful use" of electronic health records through the integration of the nursing management minimum data set. *J Nurs Adm*. 2010;40(7/8):336–343.

For more than 11 additional continuing education articles related to electronic information in nursing, go to NursingCenter.com\CE.