Issues in Mental Health Nursing, 30:720–722, 2009

ISSN: 0161-2840 print/ 1096-4673 online
DOI: 10.3109/01612840902722179

informa
healthcare

HEALTH INFORMATION TECHNOLOGY AND LITERACY COLUMN

Personal Health Records: Protecting Behavioral Health Consumers' Rights

Edited by Marilyn S. Fetter, PhD, PMHCNS-BC
Villanova University, College of Nursing, Villanova, Pennsylvania, USA

Patient-centric Personal Health Records (PHRs) are a critical companion to Health Information Technology (HIT) policy and strategy worldwide. Along with Electronic Health Records (EHRs), PHRs have been conceptualized as promoting care safety, quality, access, efficiency, and cost effectiveness (Department of Health and Human Services [DHHS], 2008). PHRs have the potential to empower health consumers to engage more actively in care and wellness activities (Kupchunas, 2007). In terms of population health, fully operationalized PHRs give epidemiologists, researchers, and policy makers vehicles to mine and analyze data; disseminate health education and alerts; access and enroll consumers in trials, pilot projects, and ongoing initiatives; and conduct program evaluation (Gunter & Terry, 2005). In order to cross the quality chasm in mental health and substance use treatment and prevention, HIT is seen as transformative (Institute of Medicine, 2006). However, the benefits of PHRs have not been well-studied. Research on EHRs has shown modest benefits offset by the cost of implementation and the need to overcome significant barriers, such as privacy and security concerns (Hillestad et al., 2005; Robert Wood Johnson Foundation, 2008). However, PHRs have received little research attention. In addition, they pose special risks, because those not institutionally based and controlled are not considered legal medical records and, thus, are not covered under most privacy laws and regulations. With its added confidentiality dimensions, mental health care poses high hurdles for full implementation of PHRs due to numerous consumer, provider, and policy issues challenging adoption. Defending behavioral consumers' rights will depend on psychiatric mental health nurses (PMHNs) and other clinicians engaging in protective legislation, policies, and practices.

Progress achieving interoperability and security is advancing the realization of a National Health Information Network (NHIN) in the U.S. and several other countries; however, difficulties overcoming privacy concerns have retarded initiatives (McBride, 2008). Providers receiving federal and state funds now realize that once a system is in place, they will be required to submit all client information into a centralized government database. Consumers will not have any control over the use of the data. In addition, the nation's Privacy Rule denies individuals the right to sue when breaches occur. In Massachusetts, which has already adopted statewide health care, these data have been released to physicians and other clinicians, insurers and their financial clearinghouses, and health systems, in full compliance with HIPAA (Health Information Portability Accountability Act) and Privacy Rule regulations. The data reported in PHRs are even more vulnerable, because HIPAA only protects covered entities, not non-institutional organizations, such as Google, Microsoft, and software vendors (Levy, 2008). Experts, as well as consumer advocates, contend that wide, unregulated, and unmonitored access violates the principle of patient-provider privacy. Further, guarded consumers engage in so-called "privacy protective behaviors," such as avoiding clinical tests and reporting. These actions compromise patient safety and thwart the achievement of the PHR's benefits (Robert Wood Johnson Foundation, 2008). When privacy is protected, the quality and reliability of health data are improved, which in turn diminishes tort-based liabilities and allows for research that can yield overall improvements in health care delivery (Hodge, Gostin, & Jacobson, 1999).

The security of electronic data worries providers, patients, and regulators. In a 2006 study by the Markle Foundation, consumers reported the following concerns: identity theft and fraud, 80%; availability to marketers, 77%; employer notification, 56%; and release to insurers, 53% (Angst, 2008). Participation in a PHR was positively correlated with education and knowledge, but survey participants expressed a willingness to relinquish privacy for better care. This finding reinforces contentions that vulnerable individuals, such as the poor and those with limited literacy, may not derive the same benefits and may experience unique access and other barriers with respect to HIT (Robert Wood Johnson Foundation, 2008). Providers, such

Address correspondence to Marilyn S. Fetter, College of Nursing, Villanova University, Nursing, 850 Lancaster Ave., Villanova, 19085 United States 850 Lancaster Ave., Villanova, PA 19085. E-mail: mfetter4@aol.com

as clinicians and health care institutions, also express privacy concerns. In Congressional testimony the American Psychiatric Association (2008) cited compelling statistics from national surveys. Approximately, two million individuals fail to seek mental health treatment due to privacy fears alone, and a fifth of all patients report withholding information for fear of disclosure. In practices, particularly solo and small group ones common in psychiatry and psychiatric nursing, patient trust can be eroded if confidentiality is perceived as threatened, but extra security provisions add to already steep costs distributed over a small group of revenue producers (American Psychiatric Association, 2008). Until 2006, federal regulations prohibited health systems from providing or underwriting HIT for practices, and there are still strict specifications that must be met for satisfying exceptions to physician self-referral rules for e-prescribing and EHRs (DHHS, 2006). The status of non-institutional PHRs is not addressed in early regulation revision notices. These factors have contributed to lagging HIT adoption rates in psychiatry (Daly, 2007; Mojtabai, 2007). While unstudied, these problems may be at play in psychiatric-mental health nursing as well (Puskar, Aubrecht, Beamer, & Carozza, 2004). Further, health systems are advised that any interfacing entity with their HIT systems leaves them open to and liable for security violations (Turisco & Kilbridge, 2000). For example, non-secure links to outside organizations or companies via Web pages, rogue employee activity that "opens" a window into the system, and consumers "correcting" their clinical data in non-firewalled PHRs are examples of potentially risky situations. Nurse managers and other health executives are encouraged to remember that protecting patients' privacy rights underscores the principle that all e-Health initiatives should support relationships between patients and providers (Harrison & Lee, 2006). While not addressing PHRs specifically, the National Association of Psychiatric Health Systems (2006) supports the implementation of HIT in behavioral health care to improve patient safety and quality of care, but has called for stricter state, local, and federal laws, statutes and regulations, in addition to financial support, to enhance the privacy and security of electronic data.

Protecting the privacy of clients using PHRs is the object of significant professional and governmental organization attention in the U.S. and abroad. In Europe and Australia, nationalized EHRs and PHRs are more limited in scope, but nevertheless, experts have noted the lack of strategies to protect against data breaches (Eurosocap, 2008). In a report to the U.S. Congress, the U.S. Government Accountability Office (2007) evaluated federal HIT privacy efforts. It found that despite the work of contractors and advisory committees representing the National Committee on Vital and Health Statistics and the American Health Information Community (AHIC), the DHHS has yet to define an overall privacy model and milestones; DHHS contends that it has established an approach (Department of Health and Human Services, 2003). Consumers and their advocates have opportunities to participate in the Consumer Empowerment and Personalized Healthcare workgroups recommended by the American Health Information Community (AHIC). These are accessible at the following respective sites: http://www.hhs.gov/healthit/ahic/consumer and http://www.hhs.gov/healthit/ahic/healthcare. Another resource is the Substance Abuse and Mental Health Services Administration (SAMHSA), which monitors federal privacy initiatives to ensure that they address specific concerns of behavioral health stakeholders, and issues reports on its Web site (2006). The National Association of Psychiatric Health Systems (2006) has called for special privacy and security safeguards that must be balanced against benefits to patient care, coordination, and safety. This group has noted the administrative and cost burden of balancing local, state, and federal privacy laws, regulations, and statutes and called for targeted adoption and privacy funding for behavioral health facilities and clinicians. Other specialized needs include: a portable yet secure PHR, data preservation guidelines, continuity of care capability, and master treatment planning accommodation for use by the full complement of the interdisciplinary treatment team. The American Nurses' Association (ANA) is developing a position statement regarding EHRs but none for PHRs has been announced; an early draft called for "correct and efficient" data collection, but revisions are expected to explicitly address privacy (ANA, 2008).

One of the biggest challenges to comprehensive national privacy protection policies and strategies for PHRs is philosophical. A choice must be made between two competing models: data "push" and data "pull" (Gunter & Terry, 2005). In the "push" approach, consumers initiate control and literally "push" the data to selected organizations. The "pull" model allows clients to consent to "pull" data into entities and uses "opt-ins" and "opouts." Conceptually as well as technically, this dilemma along with other privacy issues is complex for experts, let alone behavioral health consumers. Thus, absent national privacy policies for PHRs, psychiatric mental health nurses must take recommended interim steps. All nurses working with electronic data need to be familiar with how HIPAA regulations, the Privacy Rule, and institutional and/or practice informed consents protect and place at risk consumers and themselves. Due to the complexity of federal and state laws and regulations, institutional counsel advice is recommended for setting, reviewing, and revising existing policies. Of particular concern is the secondary use of data and patient control regarding segmenting and accessing data (Angst, 2008). "Patient Privacy Rights" (accessible at http://www.patientprivacyrights.org) and the "Health Privacy Project" (found at http://www.cdt.org/healthprivacy) are among the consumer advocacy organizations tackling these issues. The "Wired for Health Care Quality Act," which failed in Congress, included greater privacy protections (Bush, 2008). It is unclear whether future projected health legislation will tackle the problem of privacy and the PHR. In its initiative, the American Medical Informatics Association (AMIA) plans to develop a framework for the secondary use of health data that is targeting transparent policies and practices, data control versus ownership, and public awareness campaigns. Organizations are advised to take

several steps to protect patient privacy in PHRs. These include: patient education about privacy protections and their benefits, informed consent, policies, complaint procedures, opt-out provisions, vendor practices audits, and participation in national programs. "Patient Privacy Rights" offers a toolkit that addresses many of these topics, including initiating consumer-provider discussions. Another resource for consumers and providers is the World Privacy Forum (http://worldprivacyforum.org), which recommends regular medical record and payment review to counter medical identity threats and theft. Organizations are considered to have a moral duty to protect the privacy rights of vulnerable clients, such as minors, the developmentally and mentally disabled, and individuals with limited functional literacy. However, there is virtually no evidence to direct such efforts (Robert Wood Johnson Foundation, 2008). This is major research gap that PMHNs are poised and encouraged to address. With their capabilities to enable seamless continuity of care, improved consumer engagement and self-efficacy, safety and quality, and enhanced prevention, PHR will yield numerous benefits for behavioral health clients, but only if privacy barriers are surmounted. Psychiatric-mental health nurses can facilitate this advance by working within practice settings and professional organizations to educate, advocate, and investigate towards this end.

REFERENCES

American Nurses Association. (2008). Position statement review: Electronic Health Record. Retrieved November 14, 2008, from http://www.nursingworld.org/Homepage/Category/Announcements/ElectronicHealthRecordPositionStatement

American Psychiatric Association. (2008). Testimony of the American Psychiatric Association, "Cost and confidentiality: The unforeseen challenges of Electronic Health Records in small specialty practices." Retrieved October 8, 2008, from www.house/gov/smbiz/hearings/hearing-7-31-08-records/Plovnick.pdf

Angst, W. (2008). Privacy safeguards in PHR adoption. *Health Management Technology, 29*, 40–42.

Bush, H. (2008). A national IT policy proves elusive. *Hospitals & Health Networks, 82*, 32–38.

Daly, R. (2007). Access to health technology sets psychiatrists apart. *Psychiatric News, 42*(20), 11.

Department of Health and Human Services. (2003). General overview of standards for privacy of individually identifiable health information. Retrieved October 8, 2008, from http://www.hhs.gov/ocr/hipaa/guidelines/overview/rtf

Department of Health and Human Services. (2006). Physician self-referral exceptions for electronic prescribing and Electronic Health Records technology. Retrieved November 15, 2008, from http://www.cms.hhs.gov/apps/media/press/release.asp?Counter=1920

Department of Health and Human Services. (2008). Health IT data, technical standards and certification. Retrieved October 29, 2008, from http://www.hhs.healthit.gov

Eurosocap (2008). European Standards on Confidentiality and Privacy in Healthcare. Retrieved October 10, 2008, from: http://www.Eurosocap.org/eurosocap-standards.aspx

Gunter, T. D., & Terry, N. P. (2005). The emergence of national Electronic Health Record architectures in the United States and Australia: Models, costs, and questions. *Journal of Medical Internet Research, 7*(1). Retrieved November 8, 2008, from http://www.jmir.org/2005/1/e3/

Harrison, J. P., & Lee, A. (2006). The role of e-health in the changing health care environment. *Nursing Economics, 24*(6), 283–291.

Hillestad, R., Bigelow, J., Bower, A., et al. (2005). Can Electronic Medical Record systems transform health care? Potential health benefits, savings, and costs. *Health Affairs, 24*(5), 1103–1117.

Hodge, J. G., Gostin, L. O., & Jacobson, P. D. (1999). Legal issues concerning electronic health information. *Journal of the American Medical Association, 282*, 1466–1471.

Institute of Medicine. (2006). *Crossing the quality chasm. Improving the quality of health care for mental and substance-use conditions.* Washington, DC: National Academies.

Kupchunas, W. R. (2007). Personal Health Record: New opportunity for patient education. *Orthopedic Nursing, 26*, 185–193.

Levy, S. (2008). Web surfer, heal thyself: Medical files in a doctor's care have special legal protections. *Newsweek, 151*(9), 16.

McBride, M. (2008). Google Health: Birth of a giant. *Health Management Technology, 29*, 8–10.

Mojtabai, R. (2007). Use of information technology by psychiatrists and other providers. *Psychiatric Services, 58*, 1261.

National Association of Psychiatric Health Systems. (2006). *Information technology principles.* Retrieved November 1, 2008, from http://www.naphs.org/members/whatnew/documents/informationtechnology.pdf

Puskar, K. R., Aubrecht, J., Beamer, K., & Carozza, L. J. (2004). Implementing information technology in a behavioral health setting. *Issues in Mental Health Nursing, 25*, 439–450.

Robert Wood Johnson Foundation. (2008). *Health Information technology in the United States: Where we stand, 2008.* Retrieved November 15, 2008, from http://www.rwjf.org/files/publications/other/EHRReport0609.pdf

Substance Abuse and Mental Health Services Administration. (2006). Electronic Records: Health care in the 21st century. Retrieved October 7, 2008, from http://www.samsha.gov/SAMSHA_News/VolumeXIV_6/index.htm

Turisco, F., & Kilbridge, P. M. (2000). Developing a value-added web site. *Healthcare Financial Management, 54*, 40–47.

U.S. Government Accountability Office. (2007). Health information technology. Congressional Report. Retrieved October 5, 2008, from http://www.gao.gov/new.items/d07238