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
and their advocates have opportunities to participate in the
partment of Health and Human Services, 2003). Consumers
stones; DHHS contends that it has established an approach (De-
DHHS has yet to define an overall privacy model and mile-
and the American Health Information Community (AHIC), the
senting the National Committee on Vital and Health Statistics
remains the major policy, but has called for stricter state, local, and federal laws,
ternational Association of Psychiatric Health Systems (2006) has
called for special privacy and security safeguards that must be
anced 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’ As-
sociation (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 pri-
tection 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 “op-
outs.” Conceptually as well as technically, this dilemma along
with other privacy issues is complex for experts, let alone behav-
ioral health consumers. Thus, absent national privacy policies
for PHRs, psychiatric mental health nurses must take recom-
meded 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 com-
plexity of federal and state laws and regulations, institutional
counsel advice is recommended for setting, reviewing, and re-
vising 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 prob-
lem of privacy and the PHR. In its initiative, the American Med-
ical Informatics Association (AMIA) plans to develop a frame-
work for the secondary use of health data that is targeting tran-
parent policies and practices, data control versus ownership, and
public awareness campaigns. Organizations are advised to take

as clinicians and health care institutions, also express privacy
concerns. In Congressional testimony the American Psychiatric
Association (2008) cited compelling statistics from national sur-
vveys. Approximately, two million individuals fail to seek mental
health treatment due to privacy fears alone, and a fifth of all pa-
ients 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 sys-
tems 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 em-
ployee activity that “opens” a window into the system, and con-
sumers “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 pa-
ients and providers (Harrison & Lee, 2006). While not address-
ing 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,
statistics and regulations, in addition to financial support, to en-
hance the privacy and security of electronic data.

Protecting the privacy of clients using PHRs is the object
of significant professional and governmental organization at-
tention in the U.S. and abroad. In Europe and Australia, na-
tionalized EHRs and PHRs are more limited in scope, but
nevertheless, experts have noted the lack of strategies to pro-
tect against data breaches (Eurosocap, 2008). In a report to
the U.S. Congress, the U.S. Government Accountability Of-
Office (2007) evaluated federal HIT privacy efforts. It found that
despite the work of contractors and advisory committees repre-
senting 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 mile-
stones; DHHS contends that it has established an approach (De-
partment of Health and Human Services, 2003). Consumers
and their advocates have opportunities to participate in the
Consumer Empowerment and Personalized Healthcare work-

groups recommended by the American Health Information
Community (AHIC). These are accessible at the following re-
pective 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 Adminis-
tration (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 Na-
tional 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’ As-
sociation (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 pri-
tection 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 “op-
outs.” Conceptually as well as technically, this dilemma along
with other privacy issues is complex for experts, let alone behav-
ioral health consumers. Thus, absent national privacy policies
for PHRs, psychiatric mental health nurses must take recom-
meded 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 com-
plexity of federal and state laws and regulations, institutional
counsel advice is recommended for setting, reviewing, and re-
vising 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 prob-
lem of privacy and the PHR. In its initiative, the American Med-
ical Informatics Association (AMIA) plans to develop a frame-
work for the secondary use of health data that is targeting tran-
parent 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


Copyright of Issues in Mental Health Nursing is the property of Taylor & Francis Ltd and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.