

RUNNING HEAD: HEALTH LITERACY AND PRIVACY

Health Literacy and Privacy:
Consumer Confidence in Electronic Personal Health Records
Ken Bavier

N410 Issues Analysis Paper
Duke University School of Nursing
Program in Nursing Informatics

July 8th, 2005

Dr. Linda Goodwin

Introduction

The past decade has seen significant advancement in the treatment of many diseases that threaten our population. Medications have been developed to control blood pressure, slow the advancement of HIV, and cure many types of cancer. Engineers have created glucometers that require very little blood, stents that slowly release medication to prevent recocclusion, and pacemakers that can shock the heart back into a safe rhythm. While these advances are significant, none can approach the health impact that can be realized through the adoption of electronic health records (EHR). By creating an electronic version of a traditionally paper-based health record, caregivers will have access to data essential to improving care across the entire spectrum of diseases and invaluable in identifying patterns of disease that have been too subtle to detect.

Electronic health records consist of health data that is recorded and stored in a digital format. The data is easily retrieved, searched, and transmitted such that optimal care can be provided. While much of the existing EHR dialogue has dealt with the capture of data within inpatient services, new products are emerging that allow consumers to store and retain their health data in electronic Personal Health Record's (ePHR). This data would be portable and available to be used across the continuum of care throughout the life of the patient. Though the personal health benefits of such a record are apparent, there are other driving and restraining forces that must be explored to resolution. Ultimately, consumers must possess trust and confidence in the security, privacy, and usefulness of any such system. Addressing deficiencies in health and technology literacy are central to establishing consumer confidence in the use of ePHRs, and thereby gleaning the greatest benefit from their use.

Impetus for Change

The impetus for change to a longitudinal ePHR comes from many diverse arenas. One of the primary driving forces is the desire to reign in the high rate of medical errors and improve the return on our health care investment (IOM, 2001). The rapid explosion of health knowledge and medical products has made it impossible for the health care professional to be fully informed, and consequently leads to a heavy use of consultants and allied health workers to meet the needs of patients. The resulting fragmentation of the patient record and inconsistent communication between providers leads to expensive redundancies, missed treatment opportunities, poor long-term disease or wellness management, and patient dissatisfaction.

Privacy issues also surface when the paper-based record is changing hands with so many providers without any accounting for who has had the opportunity to view the data. Paper records are easily photocopied, making the theft of data very easy to execute though very hard to identify. Patient's themselves often have great difficulty exercising their right to view and comment on their health record, partly because of the multiple locations where records are maintained, and partly because of providers' uneasiness with their having access to such data. It is often easier to obtain a credit report or conduct a stock transaction in a foreign country's markets than it is to assemble one's own medical record under the current system – all this despite legal rights to do so.

While the implementation and maintenance of an ePHR system would not be without cost, the savings in reduced length-of-stays, reduction in redundant testing and prescriptions, and improved management of chronic conditions would far exceed its expense. In addition, leveraging of the consumer to partner in improving their health

could provide a psychological advantage that might be realized as a reduction of cost from visits associated with unmet emotional needs. Fostering this increased competence in one's ability to care for their own health can only strengthen the relationship of trust and confidence in our health care system, while at the same time instilling a sense of ownership and autonomy that many find lacking in our current system.

Standardization of codes and messaging schemes, a cornerstone of the HIPAA Act of 1996, makes many of these improvements possible by facilitating the mining of de-identified data across institutional boundaries. Data that is stored in a coded or tagged format is available for research and examination regardless of the entity that generated it. Fleeting are the days where each organization or practitioner will store away valuable information that will remain untouched until the next visit. Imagine the knowledge that is generated each day on paper records that will never be aggregated in a form that can be used to generate knowledge. Transitioning Americans to an ePHR would end this era of wasteful documentation and give new purpose to documenting the entirety of the care episode.

Health Literacy

Despite significant public and private initiatives, health literacy remains a significant problem across the United States. A recent IOM report stated, “nearly half of all American adults – 90 million people – have difficulty understanding and acting upon health information” (2004). They further defined health literacy as “the degree to which individuals can obtain, process, and understand the basic health information and services they need to make appropriate health decisions.” With such a large percentage of our population struggling to understand basic health care and influence the direction of their

care in the current system, we cannot expect that they will have the necessary skills to make an informed choice to have and use an ePHR. Furthermore, “persons with inadequate literacy skills come from a variety of backgrounds...[though] lack of adequate literacy is twice as common for older Americans and inner-city minorities” (Williams, Davis, Parker & Weiss, 2002). This is significant in the discussion of adopting ePHRs in that those population segments identified to have the lowest literacy rates also tend to have the greatest health care needs. Consequently, they would likely benefit the most from ePHR adoption.

Federal efforts to improve health literacy have been broad, with fundamental literacy guidelines being incorporated into the “No Child Left Behind” Bill, H.R. 107-110 (No Child Left Behind [NCLB], 2001) and the guidelines for reaching the Healthy People 2010 goal of “using communication strategically to improve health” (U.S. Department of Health and Human Services [HHS], 2000). In addition, The Agency for healthcare Research and Quality, under its Evidenced-Based-Practice Program, developed scientific information on which to base guidelines for addressing deficiencies in health literacy (<http://www.ahrq.gov/clinic/epcsums/litsum.htm>, accessed July 1st, 2005).

One of the most significant state government initiatives manifests itself in the Council of State Governments “State Official’s Guide to Health Literacy” and “Health Literacy Toolkit” (Council of State Governments, 2005) which contains documents outlining the problems of low health literacy, and outlines a program to address it at many levels, including early basic literacy, mirroring what is required in the Federal “No Child Left behind” legislation.

Private and commercial initiatives include efforts by the AMA (AMA, 2005), The Partnership for Clear Health Communication (www.askme3.org), and The Center for Health Care Strategies, Inc. (Center for Health Care Strategies, 2005) to inform patients and assist providers in addressing literacy issues.

Technology Literacy

"The digital divide becomes more critical as the amount and variety of health resources available over the Internet increase and as people need more sophisticated skills to use electronic resources. Equitably distributed health communication, resources, and skills, and a robust communication infrastructure can contribute to the closing of the digital divide and the overarching goal of *Healthy People 2010* to eliminate health disparities" (HHS, 2000). The digital divide mentioned here refers to the difference between those who have the knowledge, skills, and access to computer technology and information compared to those who do not. Access to equipment and affordable Internet service is often problematic in poor or rural populations, and no improvement in technology literacy can be expected until this situation is remedied.

Without a reduction in the levels of technology illiteracy, the increasingly complex records systems and ePHRs we use will remain out of reach or unwieldy for patients and only further contribute to the existing health disparities. At the same time, a properly employed ePHR could be a useful tool to help increase health literacy. Patients could be informed about their rights, what their responsibilities are in the maintenance of their own health, and how to seek further information about the care and direction their provider gives them at the time of enrollment.

Despite the challenges, there are many other useful resources available for patients that can increase their health literacy. Patients who have access to the Internet and understand how to navigate can access a wealth of information that can help them to

increase their health and technology literacy. There are innumerable tutorials on various computer-related issues, and many reputable web sites that provide health information, support groups, and access to research findings. Patients who are able to surf the Internet may only need to be encouraged by their provider to do some personal research and then return with questions about that which they didn't understand. Patients will feel more empowered, and providers will appreciate the effort that was taken to improve one's own health.

Current and future uses of ePHR technology for those who possess some functional technology literacy include reviewing research findings, email communication with a provider, (e-consults) virtual submission and renewal of prescriptions, and adding annotations to their ePHR. In addition, practical applications could include reminders of appointments, results of tests, and translation between languages for non-English speaking patients. Teaching materials could be tailored to the patients' diagnosis, and presented in a manner that the patient can most easily understand. Multilingual, vision-impaired, and hearing-impaired patients could select the method of learning that suited them best to maximize the learning potential.

Legal Safeguards

Legal safeguards for health information were formally established in 1996 with the creation of the Health Insurance Portability and Accountability Act (HIPAA). This Act has the expressed purpose of establishing standardized transaction codes, standard identifiers, and providing for the maintenance of privacy and security during such storage and retrieval activities (HHS HIPAA Rule). The rule is targeted to "covered entities" which include health care providers, health plans, and health care clearinghouses. Any health organization that handles personal health data in the course of providing care, storing the data generated, or processing the billing is essentially covered. Insurance companies and worker's

compensation programs are not directly regulated by the Act, nor are certain business associates of providers such as accountants, contractors, or lawyers (Gostin, 2005, p. 3016). The rule states that covered entities are required to notify the authorities if they are aware of any violation or they could be held liable themselves. The basis for this liability stems from the requirement that they sign non-disclosure agreements with these third parties, outlining the legal requirements for confidentiality. The Act also provides for civil and criminal penalties for unauthorized disclosure, and requires logs of disclosure to be maintained for possible audit. Patient consent is required for disclosure with few exceptions (law enforcement, public health and welfare), and the patient should be informed if and when any unauthorized disclosure occurred. Patients are required to be informed of their rights under HIPAA and can file a formal complaint if they suspect a violation of their rights (HHS Guidelines for reporting, N.D.).

The complexity and far-reaching impact of this Act has strained providers who are familiar with such terminology as they make adjustments to ensure compliance. Patients are most certainly struggling to understand the ramifications. In the interest of simplification, much of the information portrayed in the media and print would lead one to believe that protected health information (PHI) is secure. Unfortunately, this is not always the case. Instead, “The new federal health privacy regulation may create the illusion of legal protection where none exists” (Goldman and Hudson, 2000, p. 143). Areas of potential unintended disclosure include filling out a survey to see if you are eligible to enroll in a health study, searching an online health database to learn about a disease, and answering a questionnaire in order to get a free drug sample. Since none of these sites requires any insurance or financial information to be submitted, they are not covered entities. Many commercial web sites will operate in the grey area in order to

collect this type of data, and the uninformed or misinformed patient will be exposed to the consequences.

It is also important to note that state and local laws are supplemental to the federal regulations, and are often crafted to address shortcomings of the Act. They may be more restrictive than that which is set aside by the HIPAA rule but undo any of its provisions. As with other grey area Internet enterprises such as file sharing and pornography, it is likely that businesses restricted in their activities by local or state regulation would simply relocate to other less restrictive jurisdictions.

Ethical Considerations

Nursing Informatics (NI) professionals have a significant role in cultivating the environment that surrounds the rise of the ePHR. Strict adherence to those principles will strengthen our nurse-patient relationship and continue to afford us the luxury of being the most trusted member of the health care team.

The first ethical principle to be considered is that of beneficence, or doing what is in the best interest of the patient. This principle should be addressed in several ways, depending on the Informaticists role in the practice setting, and may involve training end-users security procedures such that patient data is not compromised. It may also involve educating oneself on legislative action so that they could provide expert testimony in support of such activity. Activities that may apply when supporting the patient's use of an ePHR might include teaching the patient about creating secure passwords, encouraging them to add annotations in areas they feel are incomplete, and guiding them to resources when they have additional questions. The correct action may also be dissuading a patient from using the PHR service if it is apparent that the risks for that

patient may outweigh potential benefits. This may be apparent with patients who have technophobia, severe privacy concerns such that they are distrustful of described security mechanisms, or simply refuse to be a party in their own care.

Nonmaleficence is the principle of doing no harm to the patient. In an ePHR environment that is data rich, this may involve assuring that security mechanisms are properly designed and configured, especially sensitive data is afforded additional safeguards, and if information is released, the patient would be notified immediately so they could limit potential damage. Examples of particularly sensitive information could include HIV status, genetic test results (and incidental findings), or previous pregnancy/abortions. Unintended disclosure of this information could be life altering and affect employment, insurability, and personal relationships. Additionally, NI professionals should also encourage the advancement of tagged data sets so disclosure of information is role-specific to the greatest extent possible. There is less risk of harmful disclosure if the disclosed data is limited to that which is needed to provide care and not revealing the entire chart at each instance.

The third ethical principle that must be considered is that of justice, or ensuring equal treatment to all patients despite their level of literacy, socioeconomic, or cultural beliefs. This principle is of paramount importance for all practicing nurses, and NI professionals in particular. As discussed earlier, significant disparities exist in the available of health care and information. Informaticists must work at alleviating this disparity by ensuring the systems they work with follow literacy guidelines. Training material should be available in multiple formats and languages to meet the needs of the patients, and time should be devoted to testing the usability of these materials to ensure

they meet the needs of the target population. Additionally, the NI practitioner could go even further by advocating for public and private monies to extend the reach of technology to underserved populations, and ensure that health and technology literacy training reaches all who are willing to learn.

The fourth and final principle discussed here is that of autonomy, or respecting the patient's right for self-determination. Autonomy is realized when providers respect the patients informed decision, and do not try to interfere or change it. Potential future challenges that may manifest themselves with regards to autonomy include the loss of ability to opt out of having an ePHR. At this point, the technological infrastructure does not exist to require it, however, the national posture with regards to cost savings and management of potential bioterrorism events may push legislation in that direction.

Role of Technology

Technology has progressed to the point that it can facilitate the aggregation of health data while preventing its unauthorized disclosure. Data tagging protocols, such as the use of XML meta tags, promise to facilitate inter and intra-organizational data sharing, increased data security, and targeted release of certain data components as warranted by the clinicians role (Simons, Mandl, & Kohane, 2004). Patients can enjoy an increased level of privacy, as compared to paper-based records, by restricting data access to that which is required to provide the dimension of care they are undergoing. Examples of this might include blocking billing information from nursing staff access, limiting the data set to allergies and diagnosis for certain x-ray or diagnostic tests, or restricting access to psychiatric notes to the psychiatrist. In the latter case, a final diagnosis with treatments (medications) prescribed may be the only portion of that data

subset that requires routine disclosure to primary care providers, not the specific session or psychotherapy notes. By tailoring data disclosure to the role requirement of the provider, unintended disclosure is prevented and the patient is protected from harm.

Current encryption and authentication methods also provide a significant improvement over the level of security afforded paper-based records. Though no encryption scheme is impervious to breach, there are many options to decrease the risk of breach to negligible levels. One of the most commonly used encryption methods is based on public key techniques introduced with the “Pretty Good Privacy” product in 1991 (Zimmerman). While this scheme was originally intended to protect email messages, new commercial products expand the coverage to corporate network messaging (PGP Product Description, 2005). PGP security is dependent on the length of a key that the user selects. The longer the key, the more difficult and unlikely it is to be breached. In this scheme, a pair of keys is generated based on a user-selected passphrase; one key is private, and maintained by the user, while the other is public and posted to a central server. Whenever someone wants to message the user, they encrypt the message using the public key. When the encrypted message arrives, the user matches up their private key and enters their passphrase to decrypt the message. Of the notable weaknesses to this technique, the greatest threat comes from the user not securing the private key from being surreptitiously copied. Once copied, all that is necessary to access the information is to install a key logger file on the users computer and record the passphrase when they type it in. At that point, the perpetrator would have unfettered access to any email messages that they intercepted. If this sounds far-fetched, consider that the FBI used this tactic to obtain Nicodemo Scarfo’s passphrase and subsequently obtain information leading to

criminal charges (United States v. Scarfo, 2001). Despite the risks, few health records would contain data significant enough to encourage these types of techniques, and system safeguards would likely identify the existence of hidden programs. Greater threats exist in the form of dummy websites (spoofing) who appear as a legitimate site in order to obtain passwords and other data. Careful attention must be paid to the URL to ensure that one is at the correct location. In addition to keylogger and spoofing exploits, simply having good security habits about what information is shared in unsecured emails, securing their home computer from unwanted intruders, and having reasonable expectations about the privacy of their casual interaction with web sites can have a significant impact on the level of security and privacy a patient can experience when using technology-enhanced health services.

Smart cards, hardware keys, and biometric identifiers have been identified as means of increasing data security for health records. New variations of smart cards are coming to market frequently as data storage technologies allow for increasingly large data sets to be maintained, and security measures to be strengthened. These cards are already making their way into the financial services sector, no doubt spurred on by recent thefts of credit card numbers and other personal data. Smart cards could be used for a number of purposes, including storage and retrieval of personal health data, authentication to web-based repositories of health information, and control of access to hospital computer systems (perhaps tailoring the user interface depending on role) (Neame, 1997). Biometric identifiers often provide a second layer of security against theft of a smart card or hardware key. They could also facilitate access to data in the event of a health crisis when the patient may be unable to give a password. A hardware

key might consist of a thumb drive that contains the access key or may contain the medical record in its entirety. Variations in patient condition may necessitate the use of multiple schemes with an organization. For instance, an elderly person may not be able to understand how to access their record if they must enter a password. They may be ideal candidates for a card/biometric combination product. A young person may not be concerned about their privacy, but rather desire quick and easy access. A thumb drive/password combination may be all that they require. A parent may request that data from multiple children be placed on one device for easy of use and storage, and that should be an option.

Conclusion

Privacy concerns remain one of the largest barriers to the widespread adoption of a longitudinal ePHR. Spurred on by failures of other industry privacy safeguards, “A majority of Internet users (60%) think that putting medical records online is a bad thing, even if they are on a secure, password-protected site” (Fox & Rainie, p.12). This occurring at the same time that 85 – 90% of surfers have used the Internet to look for health information (Fox & Rainie, p. 3, Calabretta, p. 32, Choy, Hudson, Pritts & Goldman, p.4). An August 2000 report by Susannah Fox of the Pew Internet & American Life Project states that privacy concerns are higher among Internet novices, parents, women, and older Americans. These are precisely the same demographics that stand to gain the most from ePHR adoption. Continuing efforts must be undertaken to develop legal safeguards and identify technologies that will satisfy the majority of patients’ privacy and security concerns. The convenience that consumers enjoy in accessing and analyzing other personal data can be experienced with health data if patient

privacy concerns are addressed

Health and technology literacy remain significant challenges across our country, and require a concerted effort on the part of all parties in order to successfully overcome it. Addressing disparities in health literacy remains a primary role of the NI professional in support of advancing the cause of improving the state of our health care system. The specific actions of the informatics nurse will vary depending on their specific role.

Personal action at the organizational, association, and legislative level should be considered as part of their ethical responsibility of assuring that all patients have equal access to technologically enhanced health tools. Personal enrichment activities are necessary to remain informed of changes in the security environment, legislative rules, stakeholder needs, data standards, and potential opportunities for commercial and governmental involvement in activities that could advance the goal of adoption of the ePHR. These are exciting times for Nursing Informatics. We have never had the opportunity to make such a large impact on the health of so many in such a short time as we have now.

References

- AMA Health Literacy Initiative. (N.D.). Retrieved July 1, 2005, from <http://www.ama-assn.org/ama/pub/category/8115.html>
- Calabretta, N. (2002). Consumer-driven, patient-centered health care in the age of electronic information. *Journal of the Medical Library Association*, 90(1), 32-37.
- The Center for Health Care Strategies, Inc. (N.D.). Retrieved July 1, 2005, from http://www.chcs.org/search_site3978/search_site_results.htm
- Choy, A., Hudson, Z., Pritts, J., Goldman, J. (2001, November). Exposed online: Why new federal health privacy regulation doesn't offer much protection to internet users. Retrieved July 1, 2005, from http://www.pewinternet.org/PPF/r/49/report_display.asp
- Council of State Governments. (N.D.). State official's guide to health literacy. Retrieved July 1, 2005, from <http://www.csg.org/CSG/Policy/health/health+literacy/default.htm>
- Fox, S. (2000, August 20). Trust and privacy online: Why Americans want to rewrite the rules. Retrieved July 1st, 2005, from http://www.pewinternet.org/PPF/r/19/report_display.asp
- Fox, S., Rainie, L. (2000, November 26). The online health care revolution: How the web helps Americans take better care of themselves. Retrieved July 1st, 2005, from http://www.pewinternet.org/PPF/r/26/report_display.asp
- Goldman, J., Hudson, Z. (2000). Virtually exposed: Privacy and e-health. *Health Affairs*, 19 (6).

Gostin, L. O. (2001). National health information privacy: Regulations under the health insurance portability and accountability act. *Journal of the American Medical Association*. 285(23). 3015-3021

HHS Guidelines for reporting violations of HIPAA. (N.D.). Retrieved July 1, 2005, from <http://www.hhs.gov/ocr/privacyhowtofile.htm>

HHS Healthy People 2010, Goal 11, Health Communication. (2000). Retrieved on July 1, 2005, from <http://www.healthypeople.gov/document/HTML/Volume1/11HealthCom.htm>

HHS HIPPA Rule (1996, August 12). Retrieved July 1, 2005, from <http://aspe.hhs.gov/admnsimp/pl1104191.htm>

Institute of Medicine (U.S.). Committee on Quality of Health Care in America. (2001). *Crossing the quality chasm: A new health system for the 21st century*. Washington, D.C.: National Academy Press.

Institute of Medicine (U.S.). (2004). Health literacy: A prescription to end confusion (brief). Washington, D.C.: National Academy Press.

NCLB, Public Law 107-110. (2001). Retrieved July 1, 2005, from <http://www.ed.gov/about/overview/budget/budget06/nclb/index.html>

Neame, R. (1997). Smart cards – the key to trustworthy health information systems. *The British Medical Journal*, 314, 573-585.

The Partnership for Clear Health Communication. (N.D.). Retrieved July 1, 2005, from www.askme3.org

PGP Product Description (N.D.). Retrieved July 1, 2005, from <http://www.pgp.com>

- Simons, W. W., Mandl, K. D., Kohane, I. S. (2005). The PING personally controlled electronic medical record system: Technical architecture. *Journal of the American Medical Informatics Association*, 12(1), 47-54.
- United States v. Scarfo, Criminal No. 00-404 (D.N.J.). (2001, July 30). Retrieved July 1st, 2005, from <http://www.epic.org/crypto/scarfo.html>
- Williams, M. V., Davis, T., Parker, R. M., Weiss, B. D. (2002). The role of health literacy in patient-physician communication. *Family Medicine*. 34(5), 383-389.
- Zimmerman, P. (N.D.). Retrieved July 1, 2005, from <http://www.philzimmermann.com/EN/background/index.html>