Broadband and Health Care: Legal and Policy Issues with Personal Health Records (PHR)

Digital Policy Institute
October 14, 2010
Presenters

- Sara Anne Hook, M.B.A., J.D. Professor of Informatics and Adjunct Professor of Law
  Indiana University School of Informatics, IUPUI
  317–278–7690
  sahook@iupui.edu

- Josette Jones, R.N., Ph.D. Assistant Professor
  Indiana University School of Informatics, IUPUI
  317–274–8059
  jofjones@iupui.edu
Abstract

- This session will discuss the security, privacy and accessibility of PHRs and how the 2009 ARRA stimulus provisions (HITECH Act) and the 2010 National Broadband Plan facilitate, hamper or leave gaps in the implementation of PHRs for managing health information.
- It will also highlight unsettled legal issues with PHRs and the impact of state and federal legislation and government agencies.
- We are passionate about the potential for PHRs and the empowering force they bring to health care.
- Our passion for the concept of a PHR is informed by our current work in health informatics and law, but also by our previous careers as a nurse and a librarian, wherein we were advocates of the importance of the patent’s and the public’s access to information.
1. Describe the similarities and differences between the Personal Health Record (PHR) and the Electronic Health Record (EHR).

2. Outline how the 2009 stimulus provisions (ARRA, HITECH Act) and the 2010 National Broadband Plan will impact the Personal Health Record (PHR) and where there are still gaps in what is provided in terms of oversight, privacy, security and access.

3. Discuss some additional concerns in implementing PHRs, particularly legal issues.

4. Highlight other state and federal legislation that has implications for the PHR and the roles of various government agencies in the exchange of individually identifiable health information using the PHR.
Personal Health Records (PHRs) offer significant opportunities to influence behaviors and outcomes, providing a powerful tool to assist consumers in making decisions about their health care.

Although EHRs and PHRs are similar in that they both contain health-related information about an individual, there are major differences as well, especially since PHRs are created, managed, shared and controlled by individuals rather than health care providers or institutions.
EHR is defined as:
- The aggregate electronic record on health-related information on an individual
- that conforms to nationally recognized interoperability standards and that
- can be created, managed, and consulted by authorized clinicians and staff
- across more than one health care organization.

(National Alliance for Health Information Technology, 2008)
The PHR Defined:

PHR is defined as

- An electronic record of health-related information on an individual
- that conforms to nationally recognized interoperability standards and
- that can be drawn from multiple sources
- while being managed, shared, and controlled by the individual.

(National Alliance for Health Information Technology, 2008)
Thus, for an EHR or PHR, we need

- a computer, laptop, PDA, ...
  ◦ internet access
  ◦ And information from...

- Recall that for a PHR, information can be drawn from multiple sources while being managed, shared, and controlled by the individual.

- Consumer Interest

- Provider Acceptance

- Data standards for interoperability
And a PHR may have

- a remote wireless device, such as a glucometer, scale, pacemaker...
- Self-care tracking system
- personal health library
- connection to off-site e-storage (e.g., HealthVault, Google Health, ...)
- joined a telehealth network
- And all of these will require reliable and secure high-speed network transmission capabilities,
  - Especially for rural areas
  - Especially for lower-income citizens
Core Privacy Principles

- Every information-sharing effort must provide:
  - Openness and Transparency
    - Communicate policies to participants and individuals
    - Provide privacy notices to consumers
    - Involve stakeholders in developing information sharing policies
  - Purpose Specification
    - Specify the purpose of the data collection effort clearly and make it narrowly suited to the need
Core Privacy Principles

◦ Collection Limitation and Maximization
  • Assure that only data needed for specified purposes are being collected and shared

◦ Use Limitation
  • Establish processes to ensure that data are only used for the agreed upon and stated purposes
  • Establish what data access is permitted for each user

◦ Individual Participation and Control
  • Allow individuals to find out what data have been collected and who has access, and exercise meaningful control over data sharing
  • Give individuals access to information about them, and the ability to request corrections and see audit logs.
Core Privacy Principles

- **Data Integrity and Quality**
  - Provide that data are relevant, accurate, complete and up-to-date

- **Security Safeguards and Controls**
  - Establish tools and mechanisms to provide that data are secured against breaches, loss or unauthorized access
  - Establish tools and approaches for user authentication and access

- **Accountability and Oversight**
  - Establish who monitors compliance with policies and procedures for handling breach
  - Produce and make available audit logs
Core Privacy Principles

- Remedies
  - Establish mechanisms for complaints
  - Establish remedies for affected parties to compensate for harm caused by breach

What Else is Needed for a PHR?

- “The system shall provide the ability to print a current medication list and test results”
- “The system shall employ a method to terminate sessions after a certain period of inactivity” and
- “The system shall display a privacy policy to users.”
Components of EHR and PHR

1. **Personal Health functionality:**
Functions that manage information and features related to self-care and provider based care over time.

2. **Supportive functionality:**
Functions that assist with the administrative and financial requirements associated with the delivery of health care

3. **Information Infrastructure functionality:**
Functions that ensure that the PHR or EHR provide information privacy and security, promote interoperability between PHRs and EHRs, and help make PHR features accessible and easy to use.

http://www.hl7.org/ehr/
Requirements for Both PHR and EHR

- Shared software components for data storage and retrieval
- Means to readily and securely share personal health data
- Management and ownership of data
- Comparison of standards and policies that are currently available and their policies on privacy, security and access
However...

- EHR is regulated as “Protected Health Information” under HIPAA; PHR is not legally protected
- EHR only contains information on individual’s health care events, PHR does too plus other such as health proxy, Living Will, Power of Authority, etc.
Different PHR Systems = Differences in Privacy, Security and Access

- Vender created, Clinic–Hosted (Cerner – IQHealth)
- Self–built, Hospital–hosted (myCommunity)
- Self–built research system, Institution–neutral (HealthPartners)
- Self–built, Open source (Tolven)
- Government–built, Department–specific (MyHealtheVet)
- Association–Sponsored (AHIMA – myPHR)
- Software Company created, Public used (Google Health, Microsoft HealthVault, WebMD)
Some Industry Standards Relevant to PHR Interoperability, Privacy and Security

Examples

- HL7 functional model for PHR
- HL7 RIM and data models
- HL7 Continuity of care document (CCD)
- ASTM continuity of care record (CCR)
- HITSP Consumer empowerment interoperability specifications (EMS)
- AHIP/BCBSA interoperability specification
- CCHIT–ATF PHR model for certification
Stimulus Package (ARRA) 2009
Attempt to Link PHR and EHR

Under the health IT provisions of the federal stimulus package

- Changes are made to HIPAA: improved privacy and security provisions
  - Definition of “breach”
  - Individually restricted privacy directions
  - Expanded penalties
  - Expanded obligations
    - Business associates
    - Information exchanges (RHIO, HIE)
    - Accounting for disclosures

- Consumer protection is imposed on vendors of PHR
  - Rule only applies to vendor
  - Rule does not apply to HIPAA covered entities
Stimulus Package Left Gaps

- PHR breach rule = CONFUSION
  - Rule applies to vendors of PHR
  - Rule does not apply to HIPAA covered entities
  - Rule does not apply to PHR offered by health care providers

- HITECH does not apply to non–health information

- ‘Meaningful Use’ of PHR?
Since the privacy, accessibility and security provisions of the 2009 stimulus legislation (ARRA and HITECH Act) primarily apply to facilities that handle and exchange health information, questions remain about how the stimulus provisions address the implementation of robust PHR approaches.

According to the Executive Summary of the National Broadband Plan, “although broadband-enabled health information technology (IT) can improve care and lower costs by hundreds of billions of dollars in the coming decades, the U.S. is behind many advanced countries in the adoption of technology and approximately 100 million Americans do not have broadband at home.” –will make participation in a PHR system very difficult.

Also need for more robust broadband for public libraries – as recommended in the National Broadband Plan – which is where many people access the Internet.
In terms of health information, builds on the HITECH Act of 2009, which was part of the ARRA.
One of the recommendations of the plan is to look for ways to make health information more easily available for research and outcome evaluation.
According to Davis Wright Tremain, “the Plan noted that three gaps remain: adoption, information utilization and connectivity.
The FCC also makes a bold recommendation that Congress should provide consumers with access to – and control over – their digital health care data.
Access they already have, but obtaining it is cumbersome; control they do not have under current law.”
The National Broadband Plan

“Health care: Broadband can help improve the quality and lower the cost of health care through health IT and improved data capture and use, which will enable clearer understanding of the most effective treatments and processes. To achieve these objectives, the plan has recommendations that will:

◦ Drive innovative applications and advanced analytics by ensuring patients have control over their health data and ensuring operability of data.”
◦ Goal of plan is empowered consumers – see page 207 and Recommendation 10.5
Thus addresses the need to encourage more citizens to create and utilize PHRs for their own health care needs as well as the health care needs of children, the elderly and others in their care.

Relatively low adoption of PHRs even though people use lots of other online tools – social media, e-commerce, etc.

- “PHR users tend to be younger, well-educated and have higher-than-average salaries – also impact of Kaiser in California, which provides PHRs to nearly all its patients through its KP HealthConnect portal
- Less-educated, lower-income people with multiple chronic diseases may derive the greatest benefits.
- Use is about 7% of U.S. adults, up from 2.3% in a 2008 survey.” (See Fierce EMR, Broadband could spur PHR adoption by those who most need health info.)
For Connectivity, The Plan Recommends that the FCC...

- Replace the Internet Access Fund with a Health Care Broadband Access Fund – participation and subsidies would be based on need.
- Establish a Health Care Broadband Infrastructure Fund to subsidize network deployment to health care delivery locations where existing networks are insufficient – this would include allowing funding for nursing home, hospices, long-term care facilities, off-site administrative offices and data centers and even some for-profit providers.
- Work with other agencies to align its health care programs with other federal criteria for the use of health care information technology (HITECH Act).
- Play a more prominent and sustained role in supporting the nation’s health information, including the publication of a status report every two years.
PHRs as Related to UNLOCKING THE VALUE OF DATA

- The advanced use of data in health care offers immense promise in many areas:

  4. *Empowered consumers.* Consumers are too often passive recipients of care, not accessing, understanding or acting upon their own data. Health IT applications that provide easy access and simplify vast amounts of data empower consumers to proactively manage their health. Empowered consumers better grasp their health needs, demand high-quality services and make informed choices about treatment options.
Digital health care in America is at an inflection point.
The HITECH Act should vastly improve both the capture of interoperable clinical data and consumer access to such data.
Nevertheless, a number of barriers prevent the advanced use of data to make Americans healthier for less money.
First, not all types of health data are uniformly captured and interoperable. (issue with PHRs)
Second, government regulations continue to limit consumer access to personal health data. (issue with PHRs)
There are too many barriers between consumers and their health data, including administrative, diagnostic, lab and medication data.

For example, in Alabama it can take up to 60 days to receive medical records and cost $1 per page for the first 25 pages of those records.

The Health Insurance Portability and Accountability Act (HIPAA) gave individuals the right to access their protected health information.

HITECH Act broadened this right by allowing individuals to obtain a copy of their records digitally within 96 hours of the provider obtaining the information.

Lab results, for example, may only be released to “authorized persons,” which often excludes the patient, despite their requests.
Barriers to PHR Identified in the National Broadband Plan

- Consumers can access their prescription medication lists from their treating physicians or individual pharmacies that have patient portals, but not from e-prescribing intermediaries that aggregate much of this data.
- But it is consumers’ data.
- A troubling statistic is that patients are not informed of approximately 7% of abnormal lab results.\textsuperscript{73}
- Consumers armed with the right information could do a better job managing their own health, demanding higher quality services from their providers and payors and making more informed choices about care.\textsuperscript{74}
- With seamless access to their raw health data, including lab data and prescriptions, consumers could plug the information into specialized applications of their choice (in other words, a PHR) and get personalized solutions for an untold number of conditions.
Development Related to PHRs

- Innovation within this space (including for-profit and non-profit vendors of PHRs) is occurring from the ground up and it is impossible to predict the potential of future applications.
- What is certain is that in order to maximize innovation and further personalization of health care, consumers must be able to have access to all their health care data and the right to provide it to third-party application developers or service providers of their choice.\textsuperscript{75}
- Congress should consider updating HIPAA, with suitable exceptions,\textsuperscript{76} to include consumers as “authorized persons” of their digital lab data.
- In a similar vein, barriers relevant to all other forms of health data should be examined and removed.
- Still need to address privacy, security and interoperability in order for consumers to fully embrace and utilize PHRs.
Additional Concerns in Implementing PHRs

- There are some additional concerns in the development of PHRs, particularly legal issues.
- PHR can contain other information, such as health proxy, Living Will, Power of Authority, etc.
- Privacy is a major issue with the public, particularly in the wake of high-publicity cases where personal health or financial information has been put at risk and concerns about identity theft.
- In spite of a myriad of laws related to privacy, there are still questions about coverage, compliance, overlap and gaps.
- Tension between patient privacy and need for access to patient records for research and quality control.
Privacy Law: A Brief History

- Early case law on privacy
- Famous cases: *Roe v. Wade, Loving v. Virginia, Griswold v. Connecticut*
- Fair Credit Reporting Act (FCRA) – 1970
- Privacy Act of 1974
- Family Education Rights and Privacy Act (FERPA) – 1974
- Right to Financial Privacy Act – 1978
- Privacy Protection Act of 1980
- Cable Communications Privacy Act of 1984
- Electronic Communications Privacy Act (ECPA) – 1986
- Video Privacy Protection Act of 1988
- Telephone Consumer Protection Act of 1991
Privacy Law

- Driver’s Privacy Protection Act – 1994
- Telecommunication Act of 1996
- Health Insurance Portability and Accountability Act (HIPAA) – 1996
- Children’s Online Privacy Protection Act (COPPA) – 1998
- Graham–Leach–Bliley Act (GLBA) – 1999 – also known as the Financial Modernization Act
- Sarbanes–Oxley Act of 2002
- USA Patriot Act of 2001
- Fair and Accurate Credit Transactions Act (FACTA) – 2003 – requires covered entities to take steps to monitor and address signs of identity theft – “Red Flag Rules”
Privacy and Identity Theft: Proposed Legislation – Federal

- **S.3789**: Social Security Number Protection Act of 2010 – introduced 9/15/2010
- **S.3742**: Data Security and Breach Notification Act of 2010 – introduced 8/5/2010
- **S.3579**: Data Security Act of 2010 – introduced 7/14/2010
- **S.3574**: Medicare Identity Theft Prevention Act of 2010 – introduced 7/13/2010
Other Influences on the Development of the PHR

- State and federal legislation and various government agencies will shape the role of the PHR in the exchange of individually identifiable health information.
- Indiana law as example
- Legal issues in using technology to collect consumer data
- Other government agency activities and regulations that could impact the PHR
Privacy of personal information is addressed throughout the Indiana Code, including:

With IC 24–5–24 Security Freezes for Consumer Reports, Indiana joined about 40 states that allow residents to place a freeze on their credit reports.

Reflects growing concern of citizens with protecting their personal information

Identity theft as fastest growing crime in the U.S.

Medical identity theft becoming a major concern

Medicare fraud

How might this same approach affect access to personal health information – and the willingness of consumers to provide it to yet another entity (the PHR vendor or host) beyond physicians, hospitals, insurance vendors, etc.
Health Records in Indiana

- Indiana Code IC 16–39 Health Records
  - IC 16–39–1 Release of Health Records to Patients and Authorized Persons
  - IC 16–39–1–3 Persons Entitled to Request Records
  - IC 16–39–1–4 Patient Written Consent for Release of Records
  - IC 16–39–1–5 Withholding Requested Information
  - IC 16–39–5 Release of Health Records to Third Parties and for Legitimate Business Purposes
  - IC 16–39–5–3 Provider’s Use of Records; Confidentiality; Violations
  - IC 16–39–10 Disclosure of Protected Health Information
Legal Issues in Using Technology to Collect Consumer Data

- COPPA as example
- Precautions must be taken in the online collection of personal information from children under the age of 13
- COPPA’s provisions are not applicable to information collected offline
- Applies to website operators or other online services
- Includes direct collection of information from children and indirect collection (chat rooms, member pages)
- Parental consent must be obtained – a sliding scale of consent
- Requires the posting of a privacy notice that is clearly written, understandable and easy to find on the website
Legal Issues in Using Technology to Collect Consumer Data

- Personal belief is that privacy will be the “civil rights” issue of the next decade
- Data mining technologies – “Data mining uses mathematical formulas to look for patterns in those behaviors. The results could enable the grocery store to send out targeted coupons, or, in theory, help the government decide how likely it may be that someone is linked to terrorist groups.”
- Government monitoring – email, texts, telephone calls
- Linking – what you buy – recommendations
- Personal websites, blogs, social networking, podcasts, virtual worlds – now a rich source of information for litigation – will there be a backlash with consumers reluctant to share information or selecting stronger privacy protections and settings?
Although not expressly stated, many of the provisions would encourage more robust implementation of PHRs. Encouragement for vendors (for-profit and non-profit) to create these tools. Privacy, security and interoperability remain concerns that need to be addressed. Standardization and ability to connect with EHRs, radiology departments, medical devices, pharmacies, etc. Lack of access in rural communities and by low-income citizens – and by those with chronic conditions who could benefit the most – as well as the elderly and children.
Thank You!