Averting the Collision: The Importance of Effective Privacy Doctrine to Health IT

Submission for:

The eHealth Initiative's Fifth Annual Conference, "Taking the Pulse of Health IT: A Critical Review of Progress Over the Last Five Years and Key Recommendations for Success in 2009 and Beyond."

Submission by:

William A. Yasnoff, MD, PhD
Managing Partner, National Health Information Infrastructure (NHII) Advisors
CEO, Patient Privacy Certified™
Founder, Health Record Banking Alliance
1854 Clarendon Blvd.
Arlington, VA 22201
703/527-5678
william.yasnoff@nhiiadvisors.com

Katherine L. Ball, MD, MSc.
Division of Health Sciences Informatics, Johns Hopkins University, School of Medicine
Director of Informatics, Patient Privacy Certified™
kball@jhmi.edu
(410)714-2163 Mobile

Primary Area of focus:

Addressing, Privacy and Confidentiality

Title:

Averting the Collision: The impact of privacy doctrine and the health information exchange

Abstract:

Unless privacy risks are controlled and mitigated, the benefits of HIT may not be perceived as outweighing its potential harm, making progress problematic, especially for PHR platforms. Consumer expectations are promoting new enhancements in privacy values and are consistent with the motivating use of these new technologies. Policy challenges arise as a result. Consequences of the of lack of privacy standards include decreased access to care, delayed care, and discrimination. To help address these issues, independent third-party, consumer-based privacy certification can provide patients with assurance of their personal and full control over who can access their health information.

The e-Health Initiative should develop a focus on healthcare privacy. The newest privacy developments in electronic health exchange have fundamentally altered healthcare data and record keeping practices. The legal ramifications of these shifts are largely unknown.

The Institute of Medicine (IOM) reports "To Err is Human: Building a Safer Health System" and "Crossing the Quality Chasm: A New Health System for the 21st Century" stress that soft, tactical reform "around the margins" is inadequate to address the US healthcare system's ills. These reports recommend that comprehensive reform efforts of our crisis-ridden system should focus on strategic and operational solutions for improvements in patient safety, health delivery quality, and efficiency with emphasis on the use of health information technologies (HIT) as an essential tool for achieving these goals.

Considerations of the fundamental privacy principles of personal (and protected) health information (PHI) served almost as an afterthought in many of these early scholarly and policy dialogues on HIT. It is inevitable that the increased availability of PHI that results from successful deployment of HIT will expose individuals to new and unprecedented privacy risks. As a consequence, HIT success absolutely requires the establishment of robust and effective privacy protections. Unless privacy risks are carefully controlled and mitigated, the benefits of HIT may not be perceived as outweighing its potential harm, making progress problematic.

This paper highlights a unique opportunity to promote HIT success through the creation of effective health information privacy practices. Additionally, the required development process would provide a real world example of a partnership and collaboration with an organization that values and promotes privacy as a fundamental part of its culture. The authors provide a description of one important mechanism for privacy protection for consumer driver personal health records (PHRs) in the form a high quality, comprehensive and independent privacy certification to ensure that patients' control access to their health information.

The management of electronically stored protected health information (e-PHI)[i] presents a unique set of challenges not faced by most businesses. E-PHI has several characteristics that mandate extraordinary treatment to prevent inadvertent or deliberate harm. Through the Health Insurance Portability and

Accountability Act (HIPAA),[ii] PHI is subject to added regulatory and security requirements, and the uses and potential consequences for misuse of PHI pose significant clinical, ethical and legal ramifications that may have far-reaching and significant consequences to individual patients[iii] and their families. These consequences and risks have been fairly well defined by privacy experts aware that the of lack of e-PHI privacy standards translates into decrease access to care,[iv] delayed care,[v] fear of or realized discrimination for future employment[vi] and insurability.

Privacy experts representing various perspectives from consumer,[vii] legal,[viii] informatics,[ix] and beyond[x] have recognized and described the "TPO" limitations under HIPAA and related jurisdictional law. Health and Human Services (HHS) amended the HIPAA "Privacy Rule" in August 2002 eliminating the "right of consent:"

> *"The **consent provisions…are replaced** with a new provision…that provides regulatory permission for covered entities to use and disclose protected health information for treatment, payment, healthcare operation (TPO)."*

The implications of this change, which initially appears to be a reasonable compromise for assuring the efficient functioning of health care delivery, have been slow to be recognized. While the definitions of "TPO" are spelled out in the regulations, the actual decision about whether a particular disclosure qualifies as such remains solely with the holder of the information. Since neither the patient nor any other entity is even notified about TPO disclosures and no audit trail record is required, it is not possible to determine even retrospectively whether a covered entity is following the regulatory requirements. Furthermore, the covered entity is inherently conflicted when making TPO determinations, tending to classify disclosures it perceives to be in its interest as TPO. This "trust without verification" approach does not provide any meaningful assurance of privacy or protection against abuse of the TPO consent exemption. In effect, therefore, it serves to eliminate privacy.

The recent developments in PHR platforms containing e-PHI are fundamentally shifting not only healthcare record keeping but also the industry itself. Given the fragmented environment of health information exchange in the industry, the legal and policy ramifications of this shift have not been compiled comprehensively. Further complicating the privacy issues is the fact that existing regulation is insufficient

to cover new and emerging environments containing e-PHI, including PHRs. A few of the many questions that arise and mandate attention for future policy initiatives including:

- Will interpretations of HIPAA Rules be applied directly to business associates?
- Will the HIPAA rules (or revised version) be applied to new platforms and environments in the health care marketplace (e.g. PHRs and other non-HIPAA entities)?
- Should Americans wait for legislative cycles to identify and close the HIPAA privacy gaps?
- Will new legislation support new patient access rights in relation with electronic health platforms?
- Are there preferred models of health information exchange that reduce privacy uncertainties and maximize patient controls of their data?
- How will patients have privacy assurances in new environments? And how can certification support future patient trust?

It is important to note that publicly-available PHR systems are already prohibited from releasing information to private parties without consent of the account-holder under the Federal Electronic Communications Privacy Act.[xi] Therefore, extending HIPAA to cover such systems would actually eliminate these strong existing privacy protections by introducing the TPO exception in this domain.

The e-Health Initiative can serve as a leader in the creation of comprehensive privacy guidance for the healthcare industry by formulating best practices that will have fundamental importance to and impact on the industry.

Healthcare industry leaders would strongly welcome such guidance in the privacy arena, as healthcare organizations and regional care delivery systems are traditionally unable to apply adequate resources to the task of developing and maintaining best business practices for general operations. Shrinking reimbursements will exacerbate this problem at precisely the time when more resources are needed for supporting these privacy responsibilities.

Government organizations have been established to support the reformation of the US healthcare system through HIT. The Office of the National Coordinator for Health Information Technology (ONC) provides counsel to the Secretary of HHS and leadership for the development and nationwide implementation of an interoperable HIT infrastructure. Many notable, non-government organizations (NGOs), including the e-

Health Initiative,[xii] receive market, industry, philanthropic, and government aid for their support of the long-term vision of electronic health information exchange to promote US healthcare reformation and transformation. A syndrome of irrational exuberance (caused by the seduction of technology), however, often afflicts decision makers regarding real-world ease of data exchange and feasibility of interoperability of HIT to improve the health of individuals and populations. Recent medical literature and governmental research is beginning to soften the enthusiasm of HIT as a panacea to our societal healthcare maladies.[xiii]

The e-Health Initiative has the unique intellectual and professional environment to allow for the creation of a dialogue that can ultimately be the basis for the industry's reaction to privacy issues related to e-PHI.

Solidifying the importance of comprehensive privacy principles may re-ignite the enthusiasm of HIT for the market of consumer data driven technologies. Consumer and market expectations appear to be promoting new enhancements in privacy values and are consistent with the idea of motivating use of these new technologies. Information management policies, procedures and practices for PHR vendors have not previously been specifically prepared for addressing privacy of e-PHI, and even less so for e-PHI in comprehensive HIT systems. Better privacy practices coupled with effective security measures can assure improved data provided by patients for the primary uses of healthcare delivery. Focus on patient trust and assurance of data integrity for the primary uses will ultimately improve the potential for secondary uses including medical research. Defining and incorporating privacy best practices into the healthcare systems and HIT application functionality through recommended policies, procedures and HIT enhancements might improve acceptance of HIT applications by stakeholders, leading to the salutary effects on healthcare quality of which the technology is ultimately capable.

An approach to promoting consumer trust through independent, consumer-based certification.

Patient Privacy Certified™ (PPC™) was born out of the belief that consumers' personal health information is their private property—and that privacy is essential for true innovation and progress. In partnership with the privacy advocates and organizations that value a culture of privacy, PPC is recognized as the best in class for privacy certification and organizational education. The completed certification allows the display of the PPC seal, giving patients assurance of personal and full control over who can access their health

information. Patients can easily find, review and understand the privacy policy, know how their personal health information can and cannot be used and trust that their sensitive health information is never shared without explicit permission. Patients know the organization's pledge to privacy also applies to any third party that touches their information.

Patient Privacy Certified initially collaborated with a well-recognized PHR vendor-client. The vendor-client promotes and values a culture of privacy in its health information applications. After a six-month cycle of comprehensive review of organizational policies, procedures and practices related to privacy and well as discriminatory review of PHR functionality related to privacy principles, certification was granted by the PPC Steering Committee, an independent group of consumers and consumer representatives. Certification is an iterative process and audit mechanisms are in place for ongoing monitoring. PPC services will be an integral component of a future and ongoing culture of privacy for its clients and the patients and populations they serve**.** PPC excellence is demonstrated in service delivery, quality products, and partnerships and alliances. PPC programs are distinguished by use of teams of professional privacy experts and strengthened by exceptional customer service.

In conclusion, unless effective privacy policies and principles are timely and firmly established, there will be a tremendous increase in sensitive and potential life altering e-PHI maintained by new electronic platforms, networks and exchanges with little or no regulation of its many potential uses violating basic privacy rights. Future research and development will deliver the needed tools for patients to control their sensitive data in private modes. These tools may be in the form of applications with consent management functions, strict access and comprehensive query functions supported by the ease of exchange in health record banking models.[xiv] Defining the privacy functionality of a health 'record' model in a digital environment poses challenges ideally suited for highly multidisciplinary organizations like e-HI. Patient Privacy Certified leaders recognize that a separate and distinct privacy certification process is necessary to prevent a collision at the intersection of e-privacy and e-PHI. Privacy advocates and PPC™ will continue to thoroughly address how privacy law and policy changes affect functionality requirements of HIT systems and organizations.

[i] For purposes of this paper e-PHI is defined as Protected Health Information stored or maintained in electronic form; this is a subset of PHI.

[ii] P.L. 104-191 – Sec. 1171(A) - Health Insurance Portability and Accountability Act (HIPAA) of 1996 defines protected Health Information (PHI) as "Any information in any form or medium created or received by a health provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. "

[iii] Health Information Technology: ONC Commissioned Medical Identity Theft Assessment. Available at: www.hhs.gov/healthit/privacy/identytheft.html. and
"Medical Identity Theft: The Information Crime That Can Kill You" Pam Dixon, World Privacy Forum, May 3, 2006. Available at: http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf

[iv] "Invisible Wounds of War", the RAND Corp., p. 436, (2008)

[v] 65 Fed. Reg. at 82,777 and 65 Fed. Reg. at 82,467

[vi] 65 Fed. Reg. 82,467. *(Before the amended HIPAA Privacy Rule, August,2002)*

[vii] http://www.patientprivacyrights.org/

[viii] Rothstein, Mark A.(2007) 'Health Privacy in the Electronic Age,' Journal of Legal Medicine, 28:4,487 - 501

[ix] Yasnoff WA, Peel DC, Pyles JC. Shifts in health information. N Engl J Med. 2008 Jul 10;359(2):209.

[x] The House Committee on Energy and Commerce :: Hearing , Discussion Draft of Health Information Technology and Privacy Legislation, Before the House Energy and Commerce Committee, June 8, 2008

[xi] 18 U.S.C. pt. I, ch. 121, §§ 2701-2712 (1986). (Accessed June 20, 2008, at http://www.access.gpo.gov/uscode/title18/parti_chapter121_.html)

[xii] See, eHealth Initiative's Blueprint: Building Consensus for Common Action. Available at:http://www.ehealthinitiative.org/blueprint/.; and Markle Foundation. See: http://www.markle.org/.; and The Leapfrog Group – See, http://www.leapfroggroup.org/about_us. and See, Bridges to Excellence. See: http://www.bridgestoexcellence.org/.; and National Patient Advocate Foundation - A National Network For Healthcare Reform. See http://www.npaf.org/.

[xiii] Harrison MI, Koppel R, Bar-Lev S. Unintended Consequences of Information Technologies in Health Care An Interactive Sociotechnical Analysis. J Am Med Inform Assoc 2007 September 1;14(5):542-549;
Wachter RM. Expected and Unanticipated Consequences of the Quality and Information Technology Revolutions. JAMA 2006 June 21;295(23):2780-2783;
Weiner JP, Kfuri T, Chan K, Fowles JB. "e-Iatrogenesis": The Most Critical Unintended Consequence of CPOE and other HIT. J Am Med Inform Assoc 2007 May 1;14(3):387-388;
Walker et al. EHR Safety: The Way Forward to Safe and Effective Systems. J Am Med Inform Assoc.2008; 15: 272-277; and
Ash et al. The Extent and Importance of Unintended Consequences Related to Computerized Provider Order Entry. J Am Med Inform Assoc.2007; 14: 415-423.

[xiv] Yasnoff W. Are health records banks the answer? Health Data Manag. 2008 Jan;16(1):23. and
Dimick, Chris. "Taking Medical Records to the Bank." Journal of AHIMA 79, no.5 (May 2008): 24-29.