Redefining the Health Information Management Privacy and Security Role

by Laurie A. Rinehart-Thompson, JD, RHIA, CHP; Beth M. Hjort, RHIA, CHPS; and Bonnie S. Cassidy, MPA, RHIA, FAHIMA, FHIMSS

Background

The protection of individuals' sacred medical stories and a commitment to "safeguard[ing] the confidentiality of medical records" have long been fundamental roles of the health information management (HIM) professional, inherent in the HIM profession throughout its 80-year history.[1] As the first decade of the 21st century approaches its conclusion, HIM professionals continue to carry out the responsibility of maintaining the privacy and security of patient information. However, this responsibility has become increasingly more challenging and, in fact, the role of the healthcare privacy and security professional has been likened to "standing on shifting sand."[2] As the healthcare industry continues its evolution through regulatory, technological, and program design changes, HIM professionals must redefine their role as stewards of the privacy and security of patient information. In fact, as articulated in the strategic plan of the American Health Information Management Association (AHIMA), "privacy and security of personal health information are cornerstones of HIM practice and critical elements for transition to electronic health information and information exchange."[3] This article discusses the HIM professional's role in privacy and security both historically and in light of numerous evolutionary changes and the need to extend access to patient information for purposes beyond the realm of patient care.

Legal Requirements

HIM professionals play critical roles to ensure compliance with legal mandates relevant to the privacy and security of patient information. This has proven to be challenging in light of a constantly changing legislative and regulatory environment.[4] Most notable, and of greatest familiarity to the general public, are the privacy requirements of the Health Insurance Portability and Accountability Act (HIPAA) of 1996.[5] The HIPAA privacy rule, which went into effect in 2003 for most healthcare providers, ushered in a new era of privacy compliance. Prior to the implementation of the HIPAA privacy rule, healthcare providers, frequently with guidance from HIM professionals' expertise, were bound primarily by state-specific privacy laws that often focused on highly sensitive information such as behavioral health and HIV/AIDS. Although federal privacy laws existed, they were primarily limited to the Privacy Act of 1974 as well as the protection of substance abuse information, neither of which broadly affected health information.[6, 7] Although the Privacy Act of 1974 is expansive with respect to the types of information it

regulates, it governs only federal agencies and contractors, thus effectively negating applicability to a majority of healthcare providers.[8]

Among a plethora of requirements embedded in the HIPAA privacy rule is the long-standing legal concept of preemption, which requires compliance with federal law if state law is contrary to it.[9] Although HIM professionals have dealt with the interplay between state and federal law since the profession's beginning in 1928, HIPAA continues the interplay and—in ways—complicates the process. This is due in part to exceptions to the privacy rule's preemption requirement, which allow the continued exercise of state laws, even if contrary to the privacy rule, if they serve to prevent fraud and abuse; ensure appropriate regulation of insurance and health plans; or serve a compelling need related to public health, safety, or welfare where it is determined an intrusion into privacy is warranted.[10] Additionally, preemption is excepted where a "provision of State law relates to the privacy of health information and is more stringent than a standard, requirement, or implementation specification."[11] With guidance from task forces created by states to analyze the interplay of state laws and the privacy rule, HIM professionals are charged with applying the legal complexities of preemption to daily situations involving the appropriate and lawful use and disclosure of protected health information. Given the dynamic nature of state and federal legislative and regulatory processes, this task presents a constant challenge.

RTI International, in research conducted as part of the Health Information Security and Privacy Collaboration (HISPC) project for the Office of the National Coordinator, found that the healthcare industry continues to suffer from misinterpretations of provisions and the limited reach of the HIPAA privacy rule.[12] These misinterpretations often center on aspects such as authorization, consent, patient right of access, the minimum necessary requirement, and preemption, all functions that involve the HIM professional at some level.

Often viewed as a counterpart to the HIPAA privacy rule, the HIPAA security rule first required compliance by most covered entities in 2005. This rule implements the security requirements of HIPAA. Composed of administrative, physical, and technical safeguards and applicable only to electronic health information, the security rule challenges HIM professionals to develop their expertise further into the information technology arena to ensure that electronic patient information is appropriately safeguarded.[13] As electronic systems become increasingly more powerful and complex with information being shared throughout the healthcare industry through health information exchange (HIE), the ability to prevent and monitor inappropriate access using various types of controls becomes critical.[14] Amid criticism that efforts to compel compliance with the privacy rule were not stringent enough, the final HIPAA Enforcement Rule went into effect in 2006. Creating standardized procedures and substantive requirements for investigating complaints and imposing civil monetary penalties for HIPAA violations, the Enforcement Rule sought to create a uniform compliance and enforcement mechanism to address both the privacy and security rules, among other administrative simplification provisions.[15] Still, more than five years past the HIPAA privacy rule implementation date and despite implementation of the Enforcement Rule, an October 2008 report from the Office of Inspector General (OIG) challenged ineffective enforcement and called for stronger, more regular security surveys beyond those that are complaint driven.[16] Changes in enforcement and in substantive areas of the privacy and security rules affecting consumer rights, along with requirements imposed on healthcare providers, will continue to complicate the HIM role.

The American Recovery and Reinvestment Act (ARRA), signed by President Obama on February 17, 2009, and commonly referred to at this juncture as the stimulus bill, includes $19.2 billion in provisions

for health information technology and health information management. Title XIII of the ARRA, Health Information Technology, which is cited as the Health Information Technology for Economic and Clinical Health (HITECH) Act, includes several amendments to HIPAA's privacy and security provisions.[17] Because violations and breaches of health information have occurred since the implementation of HIPAA, the need to update standards and definitions for HIT adoption has been critical. A recent study by the Institute of Medicine raised the concern that the current HIPAA privacy provisions do not provide the safeguards needed to protect the privacy of medical information nor do the measures adequately encourage research. It recommended that Congress make improvements to strike a better balance. ARRA seeks to implement this balance.[18]

The HITECH Act extends certain HIPAA provisions and penalties to covered entities and business associates, updates existing HIPAA standards for healthcare privacy and security, and includes various security breach notification requirements. Its provisions also address the minimum necessary standard, accounting of disclosures, the sale of protected health information, marketing, fundraising, electronic health records (EHRs), personal health records (PHRs), and HIPAA enforcement. Mindful of concerns about privacy and the security of electronic record systems, the HITECH Act strengthens protections of healthcare information as well. It extends the privacy and security regulations of HIPAA to health information vendors not previously covered by the law, including businesses such as Google and Microsoft, when they partner with healthcare providers to create PHRs for patients. It requires healthcare organizations to promptly notify patients when personal health data have been compromised, and it limits the commercial use of such information.[19] Breach identification and notification requirements are established for essentially any organization holding personal health information, whether or not the entity is covered by HIPAA.[20] Also of tremendous importance to the health information profession is the codification of the Office of the National Coordinator for Health Information Technology (ONC), which changes the paradigm of privacy and security efforts—particularly in the EHR arena—which had been primarily those of volunteers and the private sector.

Challenges

In addition to legal requirements that continually compel HIM professionals to redefine their roles, the advent of technology finds the HIM profession challenged as it manages information as dynamic as the healthcare industry itself. Adding to a privacy professional's role complexity are information proliferation and pervasiveness, widespread access to data with few industry or geographical standards, newfound information seekers, ungoverned health information handlers, and secondary databases—all in the midst of portability, unprecedented speeds, regulatory disparities, consumer pressures, and workflow modifications. The HIM professional's role is shifting as the healthcare industry shifts to accomplish national health reform goals for improved care quality. Since 2004, change drivers in the federal government have begun to escalate technology implementations toward EHRs and HIE through the transformation set in motion by the ONC in its National Strategic Framework Report.[21] This momentum picked up legislatively in 2009 with ARRA support for EHR adoption and expedited interoperability. Since then, the unanticipated functionality impact on information uses and disclosures has rippled beyond policies, procedures, and staff training into infrastructure and governance, technology and systems, product functions alignment, and information flow. Even the most proactive privacy professional must be postured to absorb unexpected complexities brought on by the transformation of health records from paper to electronic. Today, the consumer is at the center of healthcare transformation. While privacy is one aspect of consumer trust, evidence of lack of trust in information privacy creates an inverse relationship to moving ahead with health reform and supportive legislation. Information sharing is inextricably linked to improving patient care, but it has yet to be demonstrated whether leaps will occur or

whether change will be impeded by limited consumer trust. As a balance is sought between information availability and confidentiality, it is clear that privacy issues overlay clinical decision making in ways not clearly discernable prospectively, certainly not by those unfamiliar with the clinical relevance of withheld health information.[22] Perhaps the harm to be avoided in the Hippocratic oath could occur in unanticipated ways if wisdom and vigilance are not applied in the redesign of healthcare.

In the dilemma to define information *ownership* in today's electronic environment, *stewardship* is emerging as a replacement concept.[23] Where the reach of privacy laws falls short, and as free enterprise is a democratic right, the industry is not positioned to rein in ungoverned accountability. What is known is that information ownership, described concisely for health information students as long as HIM has been a profession, has become diffused and difficult to define.[24–26] An organization's release-of-information functions may not be optimally centralized as benefits of speed and efficiency are sought. Legal and policy interpretations become more difficult in pursuit of consistency and compliance in a decentralized environment.[27]

HIPAA's Privacy and Security rules have shared the media spotlight with reports of information breaches at the same time that federal enforcement patterns have remained gentle to encourage cooperative change by covered entities.[28–31] These same media reports show a lack of organizational action and sanction consistency for workforce compliance negligence.[32] Coupled with the perceived laxity in HIPAA enforcement, the concept of stewardship does not appear to be showing itself deserving of consumer trust in these early stages of technology use in healthcare.[33] The industry must catch up to rebuild diminishing consumer trust during this period.

Liability lines are just as foggy as information ownership. Health information organization (HIO) and HIE development challenges deal with pinning down liabilities amid shared stakeholder responsibilities.[34–38] In the big picture, privacy is at the mercy of ethical and stewardship choices on the part of all information handlers.[39] The challenge is particularly daunting when designing technology functionality that could enhance information seekers to delve further, find answers to questions not asked, and benefit from unanticipated relational information. Consumers not impeded by privacy fears are using technology for benefits that are perceived to outweigh any privacy concerns.[40] With widespread information flow extending beyond healthcare organizations to the general public, the potential problem of restricting information too little, to our detriment, certainly exists. The profession also faces the challenge of reliably proving action accountability.[41, 42]

Unlike the trends in quality care accountability (such as quality report cards, pay-for-performance, and patient safety organizations [PSOs] that provide safety in clinical error reporting), information privacy and security incidents remain closely guarded by both regulated organizations and by surveyor bodies. Openness and exposure are less likely as lessons are learned in privacy and security arenas where right and wrong, intentional and unintentional, are held in different regard. To be sure, healthcare organizations offering high-quality care do not take lightly that the greatest threats are internal, and organized crime and malicious behaviors may exploit opportunities when the industry is technology reactive rather than proactive.

Where gaps exist in national privacy requirements, states have worked independently to tighten laws in reaction to emerging threats.[43–46] Privacy application consistency in the United States has thus been made more complex as technology benefits encourage health information movement over the wire. Variation in PHR models, mediums, sources, and functionality requires advanced consumer knowledge to

sort through the benefits and the privacy implications before making a choice. If a design gives the consumer degrees of control over the PHR not equal to the EHR, which has the same source data, additional privacy inconsistencies are introduced. Privacy officials will have rollout opportunities to influence regulatory directives as national regulatory gaps are narrowed by ARRA, with evaluation of preemptive residue under the new law.

Industry stakeholders have only one choice toward technology implementation if they are to avoid being left behind in areas critical to business viability. Privacy obligations parallel technology changes yet in many clinical settings are not championed by privacy professionals who can ensure that electronic processes are protective and legal. The impetus for providers to get on board with health reform is now nudged along by strengthened federal support for EHR implementation through ARRA funding.

The scope of influence exerted by privacy leaders today and of the future reaches beyond the traditional role, stretching to demand business acumen, an ethical conscience, and social responsibility in order to protect business information assets and contribute to the larger society.[47]

Industry Privacy and Security Initiatives

Nationally, multiple healthcare privacy and security initiatives, both public and private, are taking place. They occupy important positions as privacy and security concerns increase in the midst of burgeoning interoperability and electronic exchanges of health information. Their missions are important to the HIM profession, and an understanding of their involvement in establishing health information privacy and security is imperative. Major initiatives include the ongoing work of the ONC; the 2007–2008 American Health Information Community's (AHIC) Confidentiality, Privacy, and Security Workgroup; the Certification Commission for Healthcare Information Technology (CCHIT) Privacy and Compliance Work Group and Security Work Group; the Healthcare Information Technology Standards Panel (HITSP); and the Nationwide Health Information Network (NHIN).

Codified by the ARRA as an agency within the Department of Health and Human Services, the ONC plays an instrumental role in developing and implementing an "interoperable health information technology infrastructure" nationally. It also has provided logistical support for the American Health Information Community (AHIC), a federal "advisory committee that makes recommendations to the Secretary of HHS on how to accelerate the development and adoption of health information technology and how to make health records digital and interoperable."[48] In its role, AHIC has encouraged market-led adoption and assurance of the privacy and security of those records. Both the ONC and AHIC were formed to help advance efforts toward President Bush's goal for most Americans to have access to secure EHRs by 2014.

The National eHealth Collaborative (formerly AHIC Successor, Inc.) is a public-private partnership committed to driving the development of a secure, interoperable, nationwide health information system. The National eHealth Collaborative was founded in 2008 to build on and accelerate the accomplishments of the American Health Information Community (AHIC), a federally chartered advisory committee to the U.S. Department of Health and Human Services. AHIC Successor, Inc. was established in July 2008, to develop the necessary organizational infrastructure and governance, and to manage the transition to what is now known as National eHealth Collaborative. The National eHealth Collaborative's board and membership are representative of a broad spectrum of stakeholder groups whose participation is needed to drive the rapid development and adoption of a nationwide interoperable electronic health information system, enabling the Collaborative to offer a uniquely balanced perspective and distinct capacity to effect

the changes needed to facilitate the secure and reliable exchange of electronic health information nationwide.[49, 50]

The National eHealth Collaborative (NeHC) is developing a National Prioritization Process to advance interoperability initiatives around health IT. This new process will enable multi-stakeholder collaborations that represent a broad coalition of health-related interests to identify and submit the nationwide priorities that will further advance the healthcare community's ability to provide value to consumers.[51]

Recognizing the need to certify health information technology products, including privacy and security standards, the Certification Commission for Healthcare Information Technology (CCHIT) was created in 2004 through a joint effort by AHIMA, the Healthcare Information and Management Systems Society (HIMSS), and the National Alliance for Health Information Technology. Independent, nonprofit, and federally funded, its public mission is to accelerate the adoption of health information technology throughout the United States by certifying EHR products applicable to both ambulatory and inpatient settings. A key certification criterion is the protection of the privacy of personal health information. As such, the CCHIT Privacy and Compliance Work Group identifies necessary privacy and compliance functional criteria and/or policies for development. It is further charged with addressing the EHR privacy requirements and compliance requirements in the functionality criteria. The requirements include a focus on health information privacy as related to the acquisition, use, or disclosures of one's own identifiable health data. Additionally, CCHIT's Security Work Group is responsible for advising on the security requirements for CCHIT-certified EHRs and networks.[52]

The Healthcare Information Technology Standards Panel (HITSP) "brings together the intellectual assets of over 260 organizations with a stake in health data standards to increase the interoperability of health care systems and information." Through this collaboration, a HITSP goal is to "to harmonize standards that are critical in protecting the privacy and security of health information. Following the identification of standards, implementation guides will be created by HITSP in pursuit of interoperable EHRs."[53]

The Nationwide Health Information Network (NHIN) prototype includes "the development of security models that directly address systems' architecture needs for securing and maintaining the confidentially of health data." "Each architecture capability will be used in the next steps of the NHIN to address the complex issues of authentication, authorization, data access restrictions, auditing and logging, consumer controls of information access and other critical contributions."[54]

ARRA creates a leadership structure to guide federal HIT policy through the ONC. Currently existing under executive authority, the HITECH Act enshrines the ONC in statute and greatly expands its resources. One of the national coordinator's first responsibilities will be to create a strategic plan for a nationwide interoperable health information system, a plan that must be updated annually. Two statutory committees, a Health Information Policy Committee and a Health Information Standards Committee, will advise the coordinator. An analysis of ARRA's HIT provisions can be found at http://www.ahima.org/dc. The analysis examines the provisions of ARRA specifically addressing the privacy of healthcare data.

Conclusion

Privacy and security are critical success factors in the movement toward EHR adoption. Further, protecting patient information is on the national agenda for the 21st century through continued legislative and regulatory changes as well as governmental and private initiatives. As the industry continues to change, the HIM professional is positioned to grow in the role of privacy and security advocate. HIM professionals who serve in this advocacy function are diverse, including organizational and corporate privacy officers, compliance officers, change agents in policy development, advocates for privacy and security assurances as EHR systems are implemented and demands for information become more diverse, and representatives for consumers who often distrust the systems that house their most sacred medical stories. The expansive opportunities that exist and that are being created through the ARRA allow HIM professionals to continue their long-standing commitment to patient confidentiality while also assuming leadership positions that promote the privacy and security of health information.

Laurie A. Rinehart-Thompson, JD, RHIA, CHP, is an assistant professor of clinical allied medicine at the Ohio State University in Columbus, OH.

Beth M. Hjort, RHIA, CHPS, is a professional practice resource manager at AHIMA in Chicago, IL.

Bonnie S. Cassidy, MPA, RHIA, FAHIMA, FHIMSS, is a strategic leader at the Certification Commission for Healthcare Information Technology (CCHIT) in Atlanta, GA.

Notes

1. Huffman, Edna K. *Health Information Management.* Berwyn, IL: Physicians' Record Company, 1994.
2. "Synching Up Privacy and Security." *AHIMA Today*. October 13, 2008.
3. AHIMA Strategic Plan.
4. Firouzan, Patricia Anania, and James McKinnon. "HIPAA Privacy Implementation Issues in Pennsylvania Healthcare Facilities." *Perspectives in Health Information Management* 1, no. 3 (2004): 3.
5. "Health Insurance Portability and Accountability Act of 1996." Public Law 104-191. August 21, 1996. Available at http://aspe.hhs.gov/admnsimp/.
6. 5 U.S.C. 552a.
7. 21 U.S.C. 1101-1800 and 42 U.S.C. 4541-4594.
8. Roth, Julie. "Getting 'Hip' to Other Privacy Laws, Part 1." *Journal of AHIMA* 75, no. 2 (2004): 50–52.
9. 45 CFR 160.203.
10. 45 CFR 160.203(a)(1).
11. 45 CFR 160.203(b).
12. Dennis, Jill Callahan. "What's Next for the Privacy Rule? HIPAA for All, or Something Quite Like It." *Journal of AHIMA* 79, no. 4 (2008): 24–29.
13. Quinsey, Carol Ann. "A HIPAA Security Overview." *Journal of AHIMA* 75, no. 4 (2004): 56A–56C.
14. Quinsey, Carol Ann, and Mary Brandt. Information Security—An Overview. 2003. *Journal of AHIMA.* AHIMA Practice Brief.
15. Wilkinson, Winston. The Remarks for the Twelfth National HIPAA Summit. April 10, 2006. Office for Civil Rights and Healthcare Privacy, Washington, DC. Available at http://hhs.gov/ocr/HIPAASummitPresentation041006.doc.
16. U.S. Department of Health and Human Services, Office of Inspector General. *Nationwide Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight*. October 2006. Available at http://www.oig.hhs.gov/oas/reports/region4/40705064.pdf.
17. HR 1, The American Recovery and Reinvestment Act of 2009 (ARRA). HITECH Provisions section 1301 *et seq.* Amends 42 USC section 201 *et seq* (Public Health Service Act (PHSA)) by adding Title XXX section 3000 *et seq.*
18. Institute of Medicine. "Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research." February 4, 2009. Summary available at http://www.iom.edu/?ID=61796.
19. Blumenthal, David. "Stimulating the Adoption of Health Information Technology." *New England Journal of Medicine* 360, no. 15 (2009): 1477–1479.
20. AHIMA. "Analysis of Health Care Confidentiality, Privacy, and Security Provisions of The American Recovery and Reinvestment Act of 2009, Public Law 111-5." March 2009. Available at http://www.ahima.org/dc/documents/AnalysisofARRAPrivacy-fin-3-2009a.pdf.
21. Thompson, Tommy G., and David J. Brailer. "The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care: Framework

for Strategic Action." Office of the National Coordinator for Health Information Technology, July 21, 2004.
22. Hjort, Beth. "Quality Healthcare: Can Health Information Be Both Available and Private?" *Journal of Health Care Compliance* 10, no. 5 (2008): 41–43.
23. Burrington-Brown, Jill, Beth Hjort, and Lydia Washington. "Health Data Access, Use, and Control." *Journal of AHIMA* 78, no. 5 (2007): 63–66.
24. Huffman, Edna K. *Health Information Management*. p. 30.
25. Russell, Lynda A., and Rita Bowen. "Legal Issues in Health Information Management." In Kathleen M. LaTour and Shirley Eichenwald-Maki (Editors), *Health Information Management: Concepts, Principles, and Practice*, 2nd ed. Chicago: AHIMA, 2006, pp. 239–268.
26. Dennis, Jill Callahan. "Privacy and Health Law." In Mervat Abdelhak et al. (Editors), *Health Information: Management of a Strategic Resource*, 3rd ed. St. Louis, MO: Saunders, 2007, pp. 502–539.
27. Houser, Shannon H., Howard W. Houser, and Richard M., Shewchuk. "Assessing the Effects of the HIPAA Privacy Rule on Release of Patient Information by Healthcare Facilities." *Perspectives in Health Information Management* 4, no. 1 (2007).
28. Westin, Alan F. *How the Public Views Privacy and Health Research*. Washington, DC: National Academy of Sciences, November 2007. Available at http://www.iom.edu/Object.File/Master/48/528/%20Westin%20IOM%20Srvy%20Rept%2011-1107.pdf.
29. Angst, Cory M., and Ritu Agarwal. *Overcoming Personal Barriers to Adoption when Technology Enables Information to be Available to Others*. Robert H. Smith School Research Paper, 2006. Available at http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID922075_code603680.pdf?abstractid=922075.
30. Olsen, Douglas P., Jane Karpe Dixon, Margaret Grey, Terry Deshefy-Longhi, and Jo Cecille Demarest. "Privacy Concerns of Patients and Nurse Practitioners in Primary Care—an APRNet Study." *Journal of the American Academy of Nurse Practitioners* 17, no. 12 (December 2005): 527–534.
31. Patient Privacy Rights Foundation. Health Privacy Polls. Available at http://www.patientprivacyrights.org/site/PageServer?pagename=Polls.
32. Ornstein, Charles. "Doctors Got Off Lighter in UCLA Snooping Case." *Los Angeles Times*, April 12, 2008. Available at http://articles.latimes.com/2008/apr/12/local/me-ucla12.
33. Stewart, Rachelle S. "Protective Measures for Private Health Information." *Perspectives in Health Information Management* 4, no. 5 (2007).
34. AHIMA. "Sanction Guidelines for Privacy and Security Breaches." *Journal of AHIMA* 80, no. 5 (May 2009): 57–62.
35. AHIMA e-HIM Workgroup on HIM in Health Information Exchange. "HIM Principles in Health Information Exchange." *Journal of AHIMA* 78, no. 8 (September 2007).
36. Waller, Adele. "Getting Information Rights Right: Identifying the Rights-related Issues in Health Information Exchange." *Journal of AHIMA* 77, no. 10 (November-December 2006); 28–34. Available at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_032269.hcsp?dDocName=bok1_032269.

37. Connecting for Health. The Architecture for Privacy in a Networked Health Information Environment. 2006. Available at http://www.connectingforhealth.org/commonframework/docs/P1_CFH_Architecture.pdf.
38. Foundation of Research and Education of AHIMA. *State Level Health Information Exchange Final Report Part II: Coordinating Policies That Impact Access, Use, and Control of Health Information*. Chicago: Foundation of Research and Education of AHIMA, 2008. Available at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_040349.pdf.
39. AHIMA Code of Ethics. (Revised and adopted by AHIMA House of Delegates, July 1, 2004.) Available at http://www.ahima.org/about/documents/AHIMACodeofEthics.doc.
40. PatientsLikeMe. Available at http://www.patientslikeme.com.
41. Stone, Margaret A., Sarah A. Redsell, Jennifer T. Ling, and Alastair D. Hay. "Sharing Patient Data: Competing Demands of Privacy, Trust and Research in Primary Care." *British Journal of General Practice* 55, no. 519 (October 2005): 783–789.
42. Rozen, Michael J. "Creating a Perfect Balance: The Line Between Information Gathering, Respecting Privacy." *IN Confidence* 10, no. 12 (December 2002): 4–5. Available at http://library.ahima.org/xpedio/groups/secure/documents/ahima/bok3_005244.hcsp.
43. Kwuon, Janet H., and Rachel A. Rubin. "California's New Patient Health Privacy Laws Heighten Need for HIPAA Compliance (Effective January 1, 2009)." Reed Smith LLP, 2008. Available at http://www.lifescienceslegalupdate.com/uploads/file/alert08192.pdf.
44. California Assembly Bill 1298 (AB 1298) chaptered October 14, 2007. Available at http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=74166619483+13+0+0&WAISaction=retrieve.
45. California Assembly Bill 211 (AB211) chaptered September 30, 2008. Available at http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=74100317429+10+0+0&WAISaction=retrieve.
46. California Senate Bill 541 (SB 541) chapter September 30, 2008. Available at http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=74120618057+9+0+0&WAISaction=retrieve
47. AHIMA. *On the Front Lines of Healthcare Privacy: An AHIMA Roundtable*. 2007. Available at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_033906.pdf.
48. U.S. Department of Health and Human Services. "Vision for Health IT." Available at http://healthit.hhs.gov/portal/server.pt?open=512&objID=1212&parentname=CommunityPage&parentid=14&mode=2&in_hi_userid=10741&cached=true.
49. National eHealth Collaborative. "National eHealth Collaborative Launched." Available at http://www.nationalehealth.org/ShowContent.aspx?id=249.
50. National eHealth Collaborative. Available at http://www.nationalehealth.org/.
51. Letter to AHIC Chairman Michael O. Leavitt from the AHIC Confidentiality, Privacy, and Security Workgroup, September 23, 2008. Available at http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10741_848349_0_0_18/Recommendations%20Presented%20at%20the%20September%202008%20AHIC%20Meeting.pdf
52. Certification Commission for Healthcare Information Technology. Security Work Group. Available at http://www.cchit.org/workgroups/security.

53. Available at http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_0_18/NationwidePS_Framework-5.pdf.
54. Available at http://healthit.hhs.gov/portal/server.pt?open=512&objID=1174&parentname=CommunityPage&parentid=24&mode=2&in_hi_userid=10741&cached=true.