Law and the Public's Health

This installment of *Law and the Public's Health* examines the privacy issues, and their implications for public health policy and practice, that can be expected to arise as implementation of the health information technology adoption provisions of the American Recovery and Reinvestment Act of 2009 proceeds forward.

Sara Rosenbaum, JD
Hirsh Professor and Chair
Department of Health Policy
School of Public Health and Health Services
The George Washington University Medical Center
Washington, DC

THE HEALTH PRIVACY PROVISIONS IN THE AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009: IMPLICATIONS FOR PUBLIC HEALTH POLICY AND PRACTICE

MELISSA M. GOLDSTEIN, JD

This installment of *Law and the Public's Health* is the second in a two-part series examining the health information technology (HIT) provisions contained in the American Recovery and Reinvestment Act of 2009 (ARRA, or the Act),¹ which was signed into law by President Barack Obama on February 17, 2009. Part I discusses the federal HIT legislative and regulatory infrastructure, as well as the Medicare and Medicaid HIT adoption incentives established by the Act.² This column reviews ARRA's reforms to existing laws related to health information privacy and security, particularly its revisions to the Health Insurance Portability and Accountability Act (HIPAA). The Act extends the reach of current privacy and security standards and adds new provisions related to enforcement. Following an overview, this article describes the implications of ARRA's privacy provisions for health information collection and use in public health policy and practice.

BACKGROUND

HIT adoption has been a common element of nearly every health reform proposal made in recent years because of its potential to decrease costs, improve health outcomes, coordinate care, and improve public health.³⁻⁷ In particular, HIT is considered a critical tool for improving population health by fostering more

efficient data gathering regarding the prevalence of conditions among the population; the incidence of disease; and treatment access, quality, and effectiveness.³ Electronic health record (EHR) systems could, for example, allow public health agencies to conduct post-approval surveillance of new drugs and vaccines, monitor disease and outbreak incidence, and measure health-care outcomes at community-wide levels, such as the immunization status of children and adults. At the same time, policy makers increasingly have recognized that considerations related to patient privacy and medical confidentiality will play an essential role in gaining the public trust necessary to build these systems.⁸

One of the most sweeping pieces of economic legislation ever enacted, ARRA authorizes hundreds of billions of dollars in new health and health-care spending, including more than \$49 billion in discretionary appropriations and mandatory spending to support and promote the adoption of EHRs and the diffusion of HIT. As part of a national positioning of the health-care system that will allow for far greater access and use of personal health information, the Act contains important reforms that build on previous federal health information privacy law standards.⁹ Assuring health information privacy and security has proven to be a significant dimension of HIT adoption and, for this reason, lawmakers focused on the issue in drafting ARRA.¹⁰

National opinion surveys and focus group research have shown that most consumers want their doctors to be able to access all of their health information to provide the best care. At the same time, concern about health information privacy is widespread, especially information in electronic form, because HIT has the potential to make health information far more accessible.¹¹⁻¹³ Some consumers worry that health-care

providers, health insurers, and other vendors and suppliers with access to personal health data might misappropriate or misuse personal health information,¹⁰ or that hackers will gain access to electronic systems. Others may simply view the privacy of their data as a matter of principle.¹¹ Prior to ARRA's enactment, the U.S. Government Accountability Office (GAO) issued several reports stressing the need for rapid and comprehensive federal efforts to address dimensions of health information privacy beyond those already addressed in the HIPAA privacy and security regulations.¹⁴⁻¹⁸ In addition, federal policy makers held hearings¹⁹⁻²¹ and sponsored legislation to revise and extend existing protections in certain important ways.²²⁻²⁶

ARRA builds on the substantial existing federal privacy framework by expanding its reach, strengthening certain aspects of the regulations, and increasing federal enforcement tools. At the same time, nothing fundamentally changes the ability of public health agencies to establish standards for the reporting of important public health data or their ability to use data to monitor population health, incidence of disease, or effectiveness of treatment and care.

Taken together, ARRA's provisions strengthen the level of individual control over and access to information contained in an EHR; broaden the definition of who is a business associate of covered entities and increase business associate duties; create new notification duties in the event of security breaches; place new restrictions on marketing, fundraising, and the sale of protected health information (PHI); require the development of guidelines regarding the use of limited data sets and de-identified data; and increase penalties for violations of HIPAA and add new enforcement provisions.²⁷ Most provisions took effect in February 2010, although the penalty provisions went into effect immediately upon passage.²⁸ Some provisions require implementing regulations and, thus, will take two or more years to take effect.²⁹

Individual control over and access to PHI

ARRA broadens individual control over PHI, where previously the regulations provided only a general right of access to information held by a covered entity.³⁰ The law amends existing standards to specify that when a health-care provider or other HIPAA covered entity uses an EHR containing an individual's PHI, the individual has the right to a copy of his or her record in an electronic format and to have the record sent directly to another person.³¹ In this way, the Act supports the creation of electronic personal health records (PHRs), identified by many experts as an essential step in mak-

ing personal health data more broadly accessible than is currently the case.

The Act also gives individuals more power to restrict disclosures of their PHI. Under the current Privacy Rule, providers can choose whether to agree to follow an individual's request not to disclose his or her information (but are bound by any agreement they make).³² ARRA makes provider compliance mandatory unless disclosure is required by law (e.g., by a public health notification statute). The Act thereby allows individuals to prevent other types of disclosures if the disclosure is to a health plan for purposes of carrying out payment or health care operations (individuals may not halt disclosures for treatment), *and* if the PHI pertains to a health-care item or treatment for which the provider was paid in full on an out-of-pocket basis. Thus, for example, if an individual paid cash for a sexually transmitted disease treatment, he or she could prohibit disclosure for payment or health care operations purposes but could not restrict disclosures linked to treatment. This enhanced right to restrict disclosures does not apply to de-identified information, even if the treatment for a particular patient in a data set containing information about a group of patients was paid for in cash.³¹ In states with mandatory notification statutes, even cash payment would not override the duty to treat.

Finally, under current HIPAA regulations, covered entities are required to provide an accounting of certain disclosures of PHI at an individual's request, but they do not need to account for disclosures related to treatment, payment, or health care operations.³³ ARRA expands individuals' rights to an accounting to include all disclosures made for treatment, payment, and health care operations made through an EHR during the three-year period prior to the request.³⁴ The Act does not change the existing responsibilities of covered entities regarding accountings made to public health authorities. Covered entities are generally required to provide this information if a patient asks,³³ but not if the only information disclosed is in the form of a limited data set and the covered entity has a data use agreement with the public health authority receiving the information.³⁵

Increased duties for business associates and other entities

HIPAA recognizes both "covered entities" (i.e., health plans, health-care clearinghouses, and health-care providers who transmit health information), which are directly responsible to the federal government for compliance with the Privacy and Security Rules, and

their “business associates,”³⁶ which perform activities under contract with covered entities that involve the use or disclosure of PHI and, until the passage of ARRA, were not directly responsible to the government. ARRA preserves this covered entity/business associate distinction but eliminates some of the shield for business associates, subjecting them to certain HIPAA privacy and security requirements, not just the terms of their contractual agreements with the covered entities.³⁷ The Act also imposes new requirements on vendors of PHRs and other organizations that, until now, have not been considered covered entities under HIPAA.

Under ARRA, business associates will now be required to comply directly with most provisions of the HIPAA Security Rule.³⁸ The Act does not apply the full range of HIPAA privacy standards to business associates, but does prohibit business associates from disclosing PHI outside of the terms of a HIPAA business associate contract.³⁹ The privacy and security requirements created by ARRA itself will apply to business associates (unless otherwise indicated by the law), and business associates will now be subject to the same civil and criminal penalties applicable to covered entities under HIPAA.^{40,41} These requirements will in all likelihood affect entities such as independent data registries, as well as public health authorities that, for example, have entered into a business associate agreement for the purpose of creating a limited data set.⁴²

In addition, ARRA clarifies that health information exchanges (HIEs) and other organizations that transmit PHI to a covered entity (or its business associate) and require routine access to PHI are business associates and must enter into business associate contracts with the covered entity. The same applies to vendors that contract with a covered entity to allow the covered entity to offer a PHR to patients as part of an EHR.⁴³

Finally, ARRA requires the Secretary of the U.S. Department of Health and Human Services (the Secretary), in consultation with the Federal Trade Commission, to conduct a study and submit a report to Congress on recommended privacy and security requirements for entities that are not currently covered under the law, which could be interpreted to include consumer-facing HIT tools now being created by companies such as Microsoft, Google, and WebMD.⁴⁴

Privacy and security breach notices

Although a number of states have enacted laws requiring businesses to notify consumers of security breaches in connection with personal information held in electronic databases, HIPAA has no strict notification requirement.^{45–47} ARRA amends the law to require cov-

ered entities to notify individuals whose unsecured PHI has been disclosed as a result of a privacy or security breach.⁴⁸ In certain cases, the covered entity must also notify the Secretary and the general public. If a breach is discovered by a business associate, it is required to notify the covered entity of the breach, including the identification of each individual who is reasonably believed to have been affected by the breach.⁴⁸ The new federal requirements do not preempt more demanding state notification requirements, leaving covered entities and business associates obligated to comply with both bodies of law.⁴⁹ The requirements do not apply to certain unintentional disclosures of PHI, such as those made in good faith and within the scope of employment, as long as the information is not further disclosed.⁵⁰ ARRA also applies a similar breach notification requirement on vendors of PHRs and other non-HIPAA entities.⁵¹

Restrictions on marketing and the sale of PHI

ARRA clarifies that patient consent is required for communications by a covered entity or business associate that encourage patients to purchase or use a product or service (i.e., marketing communications). Such communications remain acceptable without consent when they describe a drug or biologic that is currently prescribed for the patient and as long as the payment to the entity that does the communicating is reasonable (which the Secretary will define by regulation). Thus, for example, mail-order pharmacies would still be able to contact patients about the purchase or use of drugs prescribed to them (including, presumably, related information that gains relevance because of the underlying treatment).⁵²

Except in the area of marketing, HIPAA has not prohibited a covered entity from being paid for PHI as long as the disclosure is otherwise permitted.^{53,54} ARRA now generally prohibits a covered entity or business associate from selling patients' PHI without specific authorization. Important exceptions to the specific authorization rule include sales of databases in connection with the support of public health activities (e.g., the creation of population registries) and sales in connection with research. Thus, a physician group practice could not sell data to a general marketing firm without specific authorization from its patients, but the group could sell the data for research purposes as long as the price charged reflects the costs of preparation and data transmittal.⁵⁵

In developing regulations to carry out ARRA's restrictions on the sale of PHI, the Act specifically requires the Secretary to evaluate the impact on research or

public health activities of placing new restrictions on what holders of information can charge for access to PHI when used for public health purposes. Specifically, the Secretary is tasked with the responsibility of determining the effect of restricting holders of data from charging for more than the costs of preparing and transmitting the data.⁵⁶ Such restrictions may be imposed only if the Secretary finds that they will not impede public health activities.⁵⁷

Limited data sets and de-identified data

To address patients' privacy concerns, advocates have called for the increased use of data stripped of patient identifiers instead of fully identifiable information where it is possible to do so and still accomplish the purpose for which the data were legitimately accessed.³ Under current law, the HIPAA Privacy Rule contains an exemption for "limited data sets" (i.e., data sets stripped of certain categories of patient identifiers that, in turn, can be used pursuant to a data use agreement⁵⁸ for research, public health, and health care operations purposes without individual patient consent).²⁴ ARRA revises current law to state explicitly that covered entities will be deemed in compliance with HIPAA when they limit the PHI used, disclosed, or requested to a limited data set.⁵⁹ If it is not practicable for a covered entity to use a limited data set, the minimum necessary amount of PHI needed to accomplish the intended purpose may be used, as is the case under current law.^{60,61} De-identified information remains exempt from disclosure limits.⁵⁹

Whereas limited data sets provide a clear outline of what information can be used or disclosed by a covered entity in situations not involving direct treatment or payment, covered entities have expressed some confusion regarding how to apply HIPAA's minimum necessary standard. ARRA addresses this issue by expressing a preference for the use of limited data sets, and also by requiring the Secretary to issue guidance on what constitutes "minimum necessary," taking into consideration that the minimum necessary should encompass the information necessary to improve patient outcomes and to detect, prevent, and manage chronic disease.⁵⁹ The Secretary is also required to develop guidance on how best to implement HIPAA's requirements for the de-identification of PHI.⁶² Thus, ARRA both strengthens existing privacy protections and recognizes the need for robust data for public health practice and research purposes.

Improved enforcement

ARRA strengthens HIPAA's privacy enforcement, including new enforcement approaches, tiered penal-

ties based upon the nature and extent of a violation and the harm caused, and the empowerment of state attorneys general to bring civil suits in federal court to recover damages on behalf of states' citizens. Increased penalties for violations of HIPAA are effective immediately, while penalties for violations of ARRA's provisions will be effective in two years.^{63,64}

IMPLICATIONS FOR PUBLIC HEALTH POLICY AND PRACTICE

HIPAA largely exempts public health data from its disclosure restrictions, permitting unauthorized disclosures of PHI to public health authorities for activities including reporting; surveillance, investigations, and interventions; activities under Food and Drug Administration jurisdiction; notification of people at risk of communicable disease; and medical surveillance in the workplace. Public health authorities are thus free under HIPAA to engage in the full range of public health activities authorized by state law—depending, of course, on the successful collection, storage, and use of the personal health and behavior data held by covered entities. The foundation for the collection of public health data is public trust, which requires maintaining the privacy and security of people's sensitive health information.⁶⁵ Formulating policy surrounding health information privacy therefore requires a careful balancing between individual rights and collective goods—fostering public trust and encouraging individuals to access treatment on the one hand, and ensuring the availability of data essential for quality assurance, cost-effectiveness studies, and public health investigations on the other.⁶⁶

ARRA retains this legal structure while simultaneously expanding the privacy protections afforded by current health information privacy law. The primary question for public health authorities after ARRA's passage, then, is how the law will affect access to the information critical to performing their duties to improve public health programs and the health of populations—access that sometimes can be incomplete even under the current system. While public health agencies retain broad authority under both HIPAA and ARRA, the Privacy Rule authorizes, but does not require, covered entities to disclose data—any mandated disclosures are required by state law.

Some covered entities currently resist sharing medical data on a large scale for public health activities (e.g., outbreak investigations or syndromic surveillance) out of concern regarding the privacy of data uses, the security of data systems, or simply the administrative burden of information sharing.⁶⁷ It is possible that

these concerns could be somewhat heightened, at least in the near term, as covered entities adjust to a revised legal environment and the increased administrative burdens of ARRA's new requirements, such as expanded accountings of disclosures and notification of breaches. Although ARRA does make certain important revisions to existing law, the authority of public health agencies remains intact. In fact, the Act carefully balances its provisions that strengthen individual rights with the importance of continued and even improved availability of data for public health activities.

Under the new law, business associates of health-care providers and other entities that create or use PHI can be held directly accountable for following HIPAA's privacy and security rules, including the stricter provisions added by ARRA, whereas before the law's passage, they were accountable only to their contractual parties.³⁷ Although most of a business associate's duties under HIPAA have not changed, it is certainly possible that concern regarding stronger enforcement authority and ARRA's increased penalties for HIPAA violations could lead to some initial hesitance to report personal health and behavior data to public health agencies. These requirements will most likely affect large aggregators of data, such as independent data registries and health information exchange organizations.

The Act also requires business associate agreements for a broader variety of entities, such as HIE networks and vendors that offer a PHR through a covered entity's EHR. If these entities currently report data to public health agencies on a voluntary basis, they may hesitate to continue the practice in reaction to their new responsibilities as business associates.

ARRA strengthens individuals' control over their own data as well, including the power to restrict disclosure of PHI for purposes of carrying out payment or health care operations. Under HIPAA, providers have been able to choose whether to follow such a request, but ARRA makes compliance mandatory if the PHI pertains to a health-care item or treatment that the individual paid for completely out of pocket, and unless the disclosure is required by law (as in the case of state-mandated public health reporting) or for treatment purposes. This provision will allow the most privacy-protective individuals among us to restrict disclosure of our most sensitive health-care information—which could include treatment for mental illness, substance abuse, and sexually transmitted infections, to name a few. However, only those with the means to pay for treatment without reimbursement will be able to take advantage of the provision, and under narrowly tailored circumstances. The provision does not apply at all to de-identified information, which means that even if

the treatment for one patient in a data set containing information about a group of patients was paid for in cash, the covered entity could disclose otherwise reportable data.²⁰ In states with mandatory reporting statutes, cash payment would not override the duty to treat. As a large proportion of public health data is reported according to state mandate, availability of data for public health analysis should not be affected seriously by the requirement.

Some public health agencies will also encounter new responsibilities under ARRA. For example, an agency that operates a health clinic and provides medical care, such as human immunodeficiency virus or tuberculosis treatment, is a covered entity under HIPAA⁶⁷ and will now be responsible for ARRA's new requirements, including those regarding notification duties in the event of security breaches and providing patients with an accounting of information disclosures. The new business associate requirements will also apply to public health authorities that, for example, have entered into a business associate agreement for the purpose of creating a limited data set. Compliance with these provisions will, of course, require additional resources from the agencies, which could strain both budgets and personnel needs.

Thus, in making these revisions, ARRA balances individual rights with the needs of population health. For example, ARRA's prohibition on the sale of PHI exempts public health activities entirely from its purview. Moreover, the law specifically requires that the Secretary, in promulgating regulations that implement the provision, evaluate the impact on research or public health activities, including any conducted by the Food and Drug Administration, of restricting payment for data disclosed for public health purposes to the costs of preparing and transmitting the data.⁵⁵

ARRA also exhibits a preference for the use and disclosure of limited data sets when practicable in lieu of covered entities' reliance on the minimum necessary standard. While this provision is designed to limit the use of PHI to those situations where the more limited disclosure is insufficient, and is therefore more protective of privacy, it could also increase the amount of data available for research, public health, and health care operations purposes. As described previously, limited data sets are stripped of a number of categories of patient identifying information and can be used pursuant to data use agreements for such purposes. In addition, ARRA requires the Secretary to issue guidance on the minimum necessary standard, with special consideration paid to its inclusion of information necessary to improve patient outcomes and to detect, prevent, and manage chronic disease.

Until such guidance is issued, a covered entity's use of the limited data set will be deemed as satisfying the standard.

Finally, the Act requires that, within a year after its passage, the Secretary meet with stakeholders to issue new guidance related to how entities should comply with HIPAA's requirements for de-identification of PHI.⁶² As HIPAA places no restrictions on using de-identified data for public health and research purposes, issuing clear guidance on their proper use could expand the data available for such purposes, thereby expanding our medical knowledge and ultimately improving the public's health.⁸ The new guidelines should ensure that EHR systems include mechanisms to securely de-identify patients' records both to protect confidential medical information and make essential data available for quality assurance, cost-effectiveness studies, and public health investigations.

CONCLUSION

Congress made the adoption of HIT one of the major policy priorities of ARRA and, in so doing, expanded health information privacy. The Act strengthens the federal privacy and security standards already in place for health information while simultaneously attempting to balance policy priorities to protect and promote both individual and population health. Although public health agencies may see some initial hesitation on the part of covered entities and business associates regarding the disclosure of information as they adjust to their new responsibilities, the Act leaves intact both the authority of public health agencies and the ability of covered entities and business associates to provide essential data for public health needs.

Melissa Goldstein is an Associate Research Professor in the Department of Health Policy at The George Washington University Medical Center, School of Public Health and Health Services in Washington, D.C.

Address correspondence to: Melissa M. Goldstein, JD, Department of Health Policy, The George Washington University Medical Center, School of Public Health and Health Services, 2021 K St. NW, Ste. 800, Washington, DC 20006; tel. 202-994-4235; fax 202-994-3504; e-mail <mgoldste@gwu.edu>.

REFERENCES

1. The American Recovery and Reinvestment Act of 2009 (ARRA), Public Law No. 111-5, 123 Stat. 115 (2009 Feb 17).
2. Burke T. The health information technology provisions in the American Recovery and Reinvestment Act of 2009: implications for public health policy and practice. *Public Health Rep* 2010;125:141-5.
3. McGraw D. Legal solutions in health reform: privacy and health information technology. Washington: O'Neill Institute for National and Global Health Law; 2009. Also available from: URL: <http://www.law.georgetown.edu/oneillinstitute/projects/reform/Privacy.html> [cited 2009 Nov 13].
4. Blumenthal D. Stimulating the adoption of health information technology. *N Engl J Med* 2009;360:1477-9.
5. Goldstein MM, Blumenthal D. Building an information technology infrastructure. *J Law Med Ethics* 2008;36:709-15, 609.
6. Lurie N, Fremont A. Building bridges between medical care and public health. *JAMA* 2009;302:84-6.
7. Chaudhry B, Wang J, Wu S, Maglione M, Mojica W, Roth E, et al. Systematic review: impact of health information technology on quality, efficiency, and costs of medical care. *Ann Intern Med* 2006;144:742-52.
8. Hall B. Searching for outbreaks: public health in a digital age. *Science Progress* 2009 Jul 27 [cited 2009 Nov 13]. Available from: URL: <http://www.scienceprogress.org/2009/07/searching-for-outbreaks>
9. Rosenbaum S, Cartwright-Smith L, Burke T, Borzi P, Goldstein M. An overview of major health information technology, public health, Medicaid, and COBRA provisions of the American Recovery and Reinvestment Act of 2009. Washington: Hirsh Health Law and Policy Program, The George Washington University, 2009 Mar 18. Also available from: URL: http://www.gwumc.edu/sphhs/departments/healthpolicy/dhp_publications/pub_uploads/dhpPublication_C02EEDD2-5056-9D20-3DE547F4F83B34.pdf [cited 2009 Jul 29].
10. Goldstein M, Repasch L, Rosenbaum S. Emerging privacy issues in health information technology. In: Blumenthal D, DesRoches C, Donelan K, Ferris T, Jha A, Kaushal R, et al., editors. *Health information technology in the United States: where we stand, 2008*. Princeton (NJ): Robert Wood Johnson Foundation; 2008. p. 92-103. Also available from: URL: <http://www.rwjf.org/pr/product.jsp?id=31831> [cited 2009 Nov 13].
11. Schneider S, Kerwin J, Robins C, Dean D. Consumer engagement in developing electronic health information systems: final report. Rockville (MD): Agency for Healthcare Research and Quality; July 2009. AHRQ Publication No. 09-0081-EF. Also available from: URL: http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS_0_1248_888520_0_0_18/09-0081-EF.pdf [cited 2009 Nov 13].
12. Westin AF. Americans overwhelmingly believe electronic personal health records could improve their health. June 2008 [cited 2009 Nov 13]. Available from: URL: <http://www.connectingforhealth.org/resources/ResearchBrief200806.pdf>
13. California HealthCare Foundation. National consumer health privacy survey 2005. Oakland (CA): California HealthCare Foundation; 2005. Also available from: URL: <http://www.chcf.org/topics/view.cfm?itemID=115694> [cited 2009 Nov 13].
14. Government Accountability Office (US). Health information technology: early efforts initiated but comprehensive privacy approach needed for national strategy. Washington: GAO; January 2007. GAO-07-238.
15. Government Accountability Office (US). Health information technology: early efforts initiated but comprehensive privacy approach needed for national strategy. Washington: GAO; February 2007. GAO-07-400T.
16. Government Accountability Office (US). Health information technology: efforts continued but comprehensive privacy approach needed for national strategy. Washington: GAO; June 2007. GAO-07-988T.
17. Government Accountability Office (US). Health information technology: HHS is pursuing efforts to advance nationwide implementation, but has not yet completed a national strategy. Washington: GAO; February 2008. GAO-08-499T.
18. Government Accountability Office (US). Health information technology: HHS has taken important steps to address privacy principles and challenges, although more work remains. Washington: GAO; September 2008. GAO-08-1138.
19. Senate Judiciary Committee (US). Health IT: protecting Americans' privacy in the digital age. 2009 Jan 27 [cited 2009 Nov 13]. Available from: URL: <http://judiciary.senate.gov/hearings/hearing.cfm?id=3632>
20. Subcommittee on Health, House Committee on Ways & Means (US). Hearing on promoting the adoption and use of health information technology. 2008 Jul 24 [cited 2009 Nov 13]. Available from: URL: <http://waysandmeans.house.gov/hearings.asp?formmode=detail&hearing=642&comm=1>
21. House Committee on Energy and Commerce (US). Discussion draft

- of health information technology and privacy legislation. 2008 Jun 4 [cited 2009 Nov 13]. Available from: URL: http://energycommerce.house.gov/index.php?option=com_content&view=article&id=1382&catid=30&Itemid=58
22. Health-e Information Technology Act of 2008. H.R. 6898, 110th Cong. (2008).
 23. PRO(TECH)T Act of 2008, H.R. 6357, 110th Cong. (2008).
 24. TRUST in Health Information Act of 2008. H.R. 5442, 110th Cong. (2008).
 25. Health Information Privacy and Security Act. S. 1814, 110th Cong. (2007).
 26. Wired for Health Care Quality Act. S. 1693, 110th Cong. (2007).
 27. ARRA Title XIII Subtitle A Part 1 § 13101 (adding new Title XXX to the Public Health Service Act (42 U.S.C. 201 et seq.)), 42 U.S.C.A. § 300jj-11, and Subtitle D Part 1 §§ 13401-13424, 42 U.S.C.A. §§ 17931-17938, 1320d-6(a), 1320d-5, 17940, 17951-17953 (West, Westlaw through September 2009).
 28. ARRA § 13410(d)(4), 42 U.S.C.A. § 1320d-5 (West, Westlaw through September 2009).
 29. Office of the National Coordinator for Health Information Technology, Department of Health and Human Services (US). Health information technology. May 2009 [cited 2009 Nov 13]. Available from: URL: http://www.hhs.gov/recovery/reports/plans/onc_hit.pdf
 30. 45 C.F.R. § 164.524 (2007).
 31. ARRA § 13405, 42 U.S.C.A. § 17935 (West, Westlaw through September 2009).
 32. 45 C.F.R. § 164.522(a) (2007).
 33. 45 C.F.R. § 164.528 (2007).
 34. ARRA § 13405(c), 42 U.S.C.A. § 17935 (West, Westlaw through September 2009).
 35. 45 C.F.R. § 164.514(e) (2007).
 36. 45 C.F.R. § 160.103 (2007).
 37. 45 C.F.R. § 164.504(e)(1) (2007).
 38. ARRA § 13401, 42 U.S.C.A. §§ 17931 (West, Westlaw through September 2009).
 39. ARRA § 13404, 42 U.S.C.A. § 17934 (West, Westlaw through September 2009).
 40. ARRA § 13401, 42 U.S.C.A. § 17931 (West, Westlaw through September 2009).
 41. ARRA § 13404, 42 U.S.C.A. § 17934 (West, Westlaw through September 2009).
 42. 45 C.F.R. 164.514(e)(3)(ii) (2007).
 43. ARRA, § 13408, 42 U.S.C.A. § 17938 (West, Westlaw through September 2009).
 44. ARRA § 13424(b), 42 U.S.C.A. § 17953 (West, Westlaw through September 2009).
 45. Missouri H.B. 62, MO. Rev. Stat. 407.1500 (2009).
 46. Ark. Code Ann. § 4-110-101 et seq. (2005).
 47. Cal. Civ. Code Ann. § 1798.80 (2008).
 48. ARRA § 13402, 42 U.S.C.A. § 17932 (West, Westlaw through September 2009).
 49. ARRA § 13421, 42 U.S.C.A. § 42 USCA § 17951 (West, Westlaw through September 2009).
 50. ARRA § 13400, 42 U.S.C.A. § 17921 (West, Westlaw through September 2009).
 51. ARRA § 13407, 42 U.S.C.A. § 17937 (West, Westlaw through September 2009).
 52. ARRA § 13406, 42 U.S.C.A. § 17936 (West, Westlaw through September 2009).
 53. 45 C.F.R. § 164.501 (2007).
 54. 45 C.F.R. § 164.508(a)(3) (2007).
 55. ARRA § 13405(d), 42 U.S.C.A. § 17935 (West, Westlaw through September 2009).
 56. ARRA § 13405(d)(3)(A), 42 U.S.C.A. §§ 17935 (West, Westlaw through September 2009).
 57. ARRA § 13405(d)(3)(B), 42 U.S.C.A. §§ 17935 (West, Westlaw through September 2009).
 58. 45 C.F.R. § 164.514(e)(4) (2007).
 59. ARRA § 13405(b), 42 U.S.C.A. § 17935 (West, Westlaw through September 2009).
 60. 45 C.F.R. § 164.502(b) (2007).
 61. 45 C.F.R. § 164.514(d) (2007).
 62. ARRA § 13424, 42 U.S.C.A. § 17953 (West, Westlaw through September 2009).
 63. ARRA § 13409, 42 U.S.C.A. § 1320d-6(a) (West, Westlaw through September 2009).
 64. ARRA § 13410, 42 U.S.C.A. § 1320d-5 (West, Westlaw through September 2009).
 65. Lee LM, Gostin LO. Ethical collection, storage, and use of public health data: a proposal for a national privacy protection. *JAMA* 2009;302:82-4.
 66. Gostin LO. Privacy: rethinking health information technology and informed consent. In: *The Hastings Center. Primers: connecting American values with health reform*. Washington: The Hastings Center; 2009 Sep 30. Also available from: URL: <http://valuesconnection.thehastingscenter.org/2009/09/30/privacy-rethinking-health-information-technology-and-informed-consent> [cited 2009 Nov 13].
 67. Gostin LO. *Public health law: power, duty, restraint*. 2nd ed. Berkeley (CA): University of California Press; 2008.