The Impact of Federal Stimulus Efforts on the Privacy and Security of Health Information in California

California HealthCare Foundation

ISSUE BRIEF

May 2009

Introduction

Health privacy laws govern the use and disclosure of an individual patient's medical information. In California, health privacy involves a sometimes complex interplay between federal requirements (chiefly, regulations enacted under the Health Insurance Portability and Accountability Act of 1996 [HIPAA][1]) and state law (especially, the Confidentiality of Medical Information Act [CMIA][2]). HIPAA regulations set the baseline for medical information protection, with specific California laws expanding patient protection where they provide more stringent regulation than that provided by HIPAA.

The recently enacted economic stimulus legislation (the American Recovery and Reinvestment Act of 2009 [ARRA][3]) has now added to this mix of state and federal law. ARRA includes a number of improvements to federal health privacy law,[4] in some cases providing stronger protections than previously existed for patients in California. On certain issues, however, it is not yet clear how regulators and courts will interpret ARRA health privacy provisions and the interplay between them and California law. Moreover, however these ambiguities are ultimately resolved, significant gaps in patient protection will remain despite the improvements made to federal privacy protections by ARRA.

This issue brief analyzes the health privacy legal landscape in California before 2009 and discusses changes made by the enactment of ARRA. The brief covers the following critical provisions of health privacy law:

- Who is covered;
- Types of health information covered;
- How entities are permitted to access, use, and disclose health information;
- Patient rights, including accounting of disclosures, records access, and control over use of information for marketing;
- Patient notification in the event of a breach; and
- Enforcement of the law.

The brief also identifies a number of significant gaps in privacy protection that remain unaddressed by state and federal law and that merit further attention from policymakers.

Health Privacy Law in California Before ARRA

Until enactment of ARRA in 2009, health privacy protection in California was an amalgam of state and federal law derived most prominently from HIPAA and the California CMIA. HIPAA set the minimum standards for patient privacy, and when California law went further than HIPAA in protecting privacy, the state's stricter laws were applied. This section analyzes how the two sets of protections operated jointly in crucial aspects of patient health privacy.

What and Who Are Covered

Both HIPAA and CMIA extend privacy protections to "identifiable health information."[6] The definition of this term differs slightly under the two statutes, but in general it means any

Federal Preemption of State Laws

The legal doctrine of preemption—that is, the overriding of state law by federal law on the same subject—can be quite convoluted. However, in the case of health information privacy laws, Congress has made things relatively simple. Congress made explicit in HIPAA that the act's federal protections do not preempt state laws on the subject, and that state regulations more protective of patient rights than HIPAA's are enforceable.[5] With regard to California, this means two things: to the extent that HIPAA and CMIA provide different but not conflicting protections, both apply; and when the provisions of either law are more protective than the other's on the same matter, the more stringent rules set the legal standard. The advent of ARRA has not altered this dynamic—ARRA health privacy provisions strengthen HIPAA itself, but do not preempt stronger provisions in California law.

information that can be identified to an individual. Under both federal and state law, information that is not individually identifiable is not protected and may be disclosed without patient authorization.

Under both federal and state law, specific protections for health information in California depend on the type of entity that created or maintains the data. HIPAA directly covers only certain types of entities in the health care system:[7] providers (including physicians, hospitals, and pharmacists); health plans and other insurers; and health care clearinghouses (which perform functions such as translating data into and out of standardized formats).[8] Individuals and organizations that use health information to perform a function or service for an entity covered by HIPAA (for example, a billing agent for a hospital or physician, or a medical transcription service) are not directly covered by HIPAA, although they must enter into contractual agreements (called business associate agreements) that set parameters for their use of data.[9] California's state law protections, on the other hand, extend not only to providers, plans, and pharmaceutical companies, but also to many of their contractors.[10]

So, in this instance, the reach of the state's health data protections has been somewhat broader than that under HIPAA.

Despite broad coverage by the two set of laws, there remained significant gaps, in particular regarding entities outside of the traditional health care system that manage health data, such as Internet companies offering personal health records (PHRs). CMIA was amended in 2008 to extend health data protections to "any business organized for the purpose of maintaining medical information" that can be used by an individual or for diagnosis and treatment purposes.[11] However, it remains unclear whether this amendment will be interpreted to cover Internet companies offering PHRs because the companies may argue that they are not "organized for this purpose."

Permitted Uses and Disclosures of Health Data

Both federal and California law permit covered entities to use identifiable information for a broad range of purposes without the need to first obtain patient consent. HIPAA permits disclosures for purposes of treatment, payment, and a range of administrative functions called "health care operations,"[12] as well as under various other exceptions. Similarly, California law permits disclosures for treatment, payment, and operations, plus 23 other exceptions (including for law enforcement, public health, quality assurance, licensing, and disease management).[13]

Further, HIPAA has always limited access, use, and disclosure of health information to the "minimum necessary" needed to accomplish the particular purpose (except in the case of treatment, and a few other categories of uses and disclosures, such as those made pursuant to patient authorization or those authorized by law).[14]

Express patient authorization is required under federal and state law for any access to or disclosure of records not covered by one of the legally permissible uses. This includes the use of individually identifiable information

for marketing purposes,[15] although (as further discussed below) the definition of "marketing" results in this protection being less meaningful than it could be. In addition, federal and state law provide extra protection for substance abuse treatment records,[16] and in California there is special protection for HIV test results.[17] Separate written authorization is also required under both HIPAA and state law for disclosure of psychotherapy notes because such notes are considered to be highly sensitive.[18]

Patients' Right to Know

One element of the right to privacy is patients' ability to find out who has obtained medical information from their records. California law does not require entities holding records to make available to patients an accounting or "audit trail" of disclosures, but HIPAA does include such a right, albeit a limited one. Under HIPAA, patients may ask covered entities for an annual report of disclosures from their records going back six years prior to the request.[19] However, this right was significantly limited by the fact that (prior to ARRA amendments; see below) entities were not required to account for most routine disclosures, such as for treatment, payment, or health care operations.[20]

Patients' Access to Their Records

In general, both state and pre-ARRA federal law provided residents of California with the right to access their medical records (with some public policy exceptions).[21] HIPAA allows entities to assess reasonable charges for copies of the records; in California, these costs are up to 25 cents per page for print records and 50 cents per page for microfilm, plus reasonable clerical fees.[22] California state law requires that requests for copies be fulfilled within 15 days.[23]

Use of Information for Marketing Purposes

Although both federal and state law require prior written authorization from patients before their identifiable information can be used for marketing purposes, the laws include a number of exceptions that frequently result in the use of patient personal information for marketing purposes without prior consent.[24] Neither federal nor state law permits outside parties to purchase identifiable data so that they can directly market products or services to patients. However, both sets of laws permit outside companies to pay health care entities to send certain health-related marketing communications on their behalf without the need to first obtain authorization. Excepted communications include those that:

- Describe products or services that are part of health plan benefits;
- Are for purposes of facilitating treatment (such as a communication that reminds a patient to refill a medication or to follow a specific care plan); and
- Are for case management or care coordination, or identify alternative treatments, therapies, providers, or facilities.[25]

California law gives patients the right to opt-out of receiving such "remunerated communications" when the communications are specifically tailored to the individual.[26]

Notification of Breach

Before ARRA modification, HIPAA did not require that individuals be notified if their health information was breached. California, on the other hand, was the first state to enact a breach notification law that applied to computerized personal information.[27] This law was amended in 2008 to extend the breach notification requirements to electronic medical and health insurance information. The law requires that a patient be notified when there has been a breach regarding health information that is not secured through encryption. For example, if a laptop containing non-encrypted patient

medical files is stolen and the health information of those patients is breached (acquired by an unauthorized person), California law requires that the patients be notified.

Enforcement of HIPAA

HIPAA includes provisions for enforcement, but since the inception of its privacy rules in 2003, the federal government has failed to make aggressive HIPAA enforcement a priority. In fact, no civil monetary penalty for a privacy violation has ever been assessed against any entity covered by HIPAA,[28] and although HIPAA regulations include authority for compliance audits, this authority has rarely, if ever, been used. Moreover, a legal memorandum by the Bush Administration Justice Department purported to limit the scope of HIPAA's criminal liability provisions, stating that only entities and not individuals could be prosecuted under the statute.[29]

In contrast, California law gives governmental authorities greater legal power to enforce state health privacy rules. The state Attorney General, a city attorney, county counsel, or district attorney may bring a civil action to enforce CMIA. In addition, individuals may sue for damages arising from any negligent release of confidential information.[30]

California law also requires certain health facilities to affirmatively prevent unauthorized access to medical information and imposes a duty to report such improper access to the Department of Public Health (DPH) within five days of an occurrence.[31] DPH is authorized to impose mandatory fines. Further, the California Office of Health Information Integrity (CalOHII) has authority to establish rules that enforce the state's health privacy laws, and DPH may delegate to CalOHII its authority to impose fines and other sanctions for unauthorized access to records.[32]

ARRA Strengthens Protections for Californians

With a few exceptions discussed above, HIPAA has been the weaker partner in the combine of federal-state health privacy protections in California. However, the passage of ARRA strengthened HIPAA in many respects, and now federal law provides protections for health information that are often equal to or stronger than those provided by CMIA. Unless specifically noted below, these new federal protections go into effect on February 18, 2010.

Who Is Covered

ARRA makes key provisions of HIPAA privacy and security rules directly applicable to "business associates" (most contractors) of covered health care entities.[33] ARRA also provides that HIPAA civil and criminal penalties may be directly assessed against these contractors.[34] This change closes a significant loophole in HIPAA coverage and enforcement, extending HIPAA accountability further down the chain of holders of health data.

In addition, ARRA clarifies that entities such as regional health information organizations (RHIOs) and health information exchanges (HIEs) are "business associates" covered by HIPAA, extending accountability to these new e-health entities.[35] California state health privacy laws were already enforceable against some contractors, but to the extent that HIPAA provides greater protections, in many cases now such contractors can be held directly accountable for complying with those stronger laws.[36]

As discussed below in the section on continuing gaps in privacy protection, the extent to which personal health record (PHR) vendors—including major companies such as Microsoft and Google—have to comply with either federal or state health privacy laws remains uncertain. ARRA makes them "business associates," and hence covered by the law when they enter into certain contractual arrangements with health care entities,[37] but it is unclear how that provision will be interpreted by federal regulators and courts. (Federal law does now

require them, whether or not they are business associates, to notify individuals in the event of a breach of their health information.) California law was amended recently to extend state law coverage to some PHR vendors (as noted above), but it is also unclear how this amendment will be interpreted.

Permitted Uses and Disclosures of Health Data

ARRA did not change the baseline HIPAA rules allowing for access, use, and disclosure—without patient consent—of identifiable health information for treatment, payment, and health care operations. However, the new law might change the amount of data that may be used or disclosed for routine purposes such as payment and health care operations. ARRA directs the U.S. Secretary of Health and Human Services (HHS) to develop guidance on what constitutes "minimum necessary," so as to give entities a clearer understanding of how to limit the amount of clinical data, or identifying information attached to data, that is accessed or disclosed for non-treatment activities.[38] Until this guidance is issued, ARRA strongly encourages entities to use a "limited data set"—health information stripped of almost all personal identifiers, including name, address, Social Security number, phone, and e-mail addresses—for routine, non-treatment purposes.[39] ARRA accomplishes this by deeming entities to be in compliance with the minimum standard if they use a limited data set. However, activities that cannot be accomplished with such a limited data set may still be conducted using identifiable data, subject to the requirement to use the minimum amount of data necessary to do so.

ARRA also allows individuals to prevent the disclosure of health data to their health plan regarding care for which they fully pay out of pocket.[40] The provision was likely intended to address the health insurance discrimination concerns of persons with particularly sensitive health conditions. However, such segregation of data may be difficult to implement, and this right can only benefit those who can afford to pay for their own care.

Patients' Right to Know

ARRA marks a major advance in the transparency of health care data disclosures. The new law makes a significant change in the HIPAA requirement to provide patients with an accounting or audit trail of disclosures from their records. Entities using "electronic health records" will have to provide an accounting or audit trail that specifically includes disclosures for such routine purposes as treatment, payment, and health care operations.[41] Such an accounting is much broader than the one required under current HIPAA rules, although it only has to cover the previous three-year period (instead of six).

ARRA also clarifies the right of patients to receive electronic copies of their medical records. The existing HIPAA right required that the copy be provided in the "form or format requested," as long as the copy was "readily producible" in that format.[42] However, ARRA specifies that entities using "electronic health records" must provide patients with an electronic copy on request (without the "readily producible" caveat).[43] Further, an individual can have that electronic copy sent directly to someone else or to a personal health record account. Individuals can only be charged for the labor costs associated with generating an electronic copy, which suggests that the permissible per-copy charges in California state law might no longer apply.

It should be noted that the true reach of these provisions will depend on how the term "electronic health record" is interpreted by federal regulators.[44] Some consumer advocates have expressed concerns that the definition may be too narrow, while some industry stakeholders are concerned that the definition may be too broad and would give access to non-clinical and purely administrative portions of records. The new disclosure rule does not go into effect for several years (2011 at the earliest), and before then HHS will need to clarify the provision through the adoption of technical standards and regulations.

Use of Information for Marketing Purposes and Sales of Personal Health Information

ARRA attempts to help patients more effectively prevent the use of their personal information for marketing purposes. Specifically, ARRA amends HIPAA rules to require authorization for most health-related communications when they are "remunerated" by an outside entity.[45] However, there are exceptions to this new protection. Even if there is outside payment, a communication is not considered marketing (and therefore does not require prior authorization) if it describes a drug or biologic that is currently prescribed for, or administered to, the individual, as long as payment for the communication is "reasonable" (to be determined by the HHS Secretary through regulations).[46] Also, the prohibition on remuneration does not extend to payment for "treatment purposes."[47] Because the definition of "treatment" in the HIPAA regulations is broad and includes care coordination and management, this rule could result in individual health information being used by health entities, without prior authorization, to send targeted health communications paid for by outside parties. Under California law, the right to opt out of such targeted communications still applies, but patients have to see, then act on, the opt-out notice for it to have any effect.

ARRA also prohibits entities covered by HIPAA from receiving payment, either direct or indirect, in exchange for identifiable health data unless they have a valid authorization from the subject individual.[48] This prohibition does not apply when payment is exchanged for health data for public health or treatment purposes or when a health care entity is changing ownership. There is also a research exception, as long as payment to the entity providing the data "reflects the cost of preparing and transmitting the data."[49] HHS must issue regulations by August 18, 2010 to carry out this new prohibition; in doing so, the agency must pay particular attention to how a restriction on payment for health data affects the use of such data for public health and research activities.

Notification of Breach

ARRA enacted breach notification requirements that, for the most part, are more stringent than California law. ARRA requires entities covered by HIPAA to notify individuals in the event of either unauthorized disclosures of health information to outside third parties or unauthorized insider access to information.[50] In this context, access or disclosure of health information is unauthorized if it is not permitted by HIPAA or not authorized by the patient (in cases where patient authorization is required). Covered entities, such as hospitals, physicians, and plans, must directly notify individuals of any breaches; business associates of a covered entity must notify that entity, which then must notify the individual. Breach of information that cannot be read or accessed because it is protected by a secure technology or methodology—such as encryption—approved by the HHS Secretary does not trigger a notification obligation.[51]

Vendors of PHRs, and of the applications that interact with such PHRs or are offered to individuals with PHR accounts, also must notify individuals in the event of a breach.[52] For these tools, which often are patient-controlled, the standard for breach notification is different: Individuals must be notified if unsecured information is acquired from their PHR without their authorization.[53]

ARRA specifies how breach notices must be sent and what information they must contain, including how the breach occurred and what actions have been taken in mitigation, as well as contact information. All breaches must be reported to federal authorities, and an entity that incurs a breach that affects 500 or more persons must notify prominent media outlets serving the state or area where the breach occurred.

These new federal breach notification provisions are broader in scope and more stringent than California law, except in one respect. Under ARRA, notification of

breach must be provided as soon as possible, and no later than 60 days after discovery of the breach. In California, entities covered by Health and Safety Code section 1280.15, which includes certain clinics, health facilities, home health agencies, and hospices, have only five days to notify individuals affected by the breach. This could be a challenge for these providers, as the new federal notification rules require that more details be included in the breach notice.

The breach notification provisions of ARRA applicable to entities covered by HIPAA and their business associates are administered by HHS; those applicable to PHR vendors not covered under HIPAA, and the companies offering Internet-based applications that interact with PHRs, are administered by the Federal Trade Commission (FTC). The breach notification provisions go into effect before other provisions of ARRA and are to be implemented by September 18, 2009.

The addition of breach notification requirements to HIPAA, and the extension of notification requirements to HIPAA business associates, PHR vendors, and other health entities not covered by HIPAA, represent important advances in the transparency of electronic record systems and could help prompt improvements in health record security.

Enforcement of HIPAA

ARRA made a number of improvements to HIPAA enforcement. Perhaps most significantly, state attorneys general are now expressly authorized to enforce HIPAA, in addition to their authority to enforce state privacy laws.[54] Other improvements to HIPAA enforcement include:

- Establishing a hierarchy of civil monetary penalties based on the egregiousness of a violation, and an overall increase in the penalty amount that can be imposed: up to a maximum of $50,000 per violation, and $1.5 million per year for repeat violations of the same offense.[55] These new penalties apply to violations that occur after the date of ARRA's enactment (February 17, 2009). Authorities still have the ability to take corrective action without imposing monetary penalties, except in instances where the violation constitutes willful neglect of the law, in which case a monetary penalty is mandatory.[56]
- Extending civil and criminal liability to business associates of entities covered under HIPAA.[57]
- Clarifying that criminal penalties can be assessed against individuals, such as employees of entities covered by HIPAA, who intentionally violate federal privacy and security rules.[58]
- Requiring HHS to develop and implement, within three years, a methodology for providing individuals aggrieved by a HIPAA violation with a percentage of any penalties or monetary settlements collected.[59]
- Requiring HHS periodically to conduct audits for compliance with HIPAA rules.[60]

Significant Remaining Gaps in Health Information Privacy

Although ARRA strengthened federal protections for health information, and California state law continues to provide even more stringent protective regulation in a number of critical areas, the federal-state combination still falls short of the comprehensive framework needed to build public trust in the health care system's information privacy and security, and particularly in electronic health information exchanges. In addition, effective implementation of the new ARRA provisions will require major effort by both federal and state regulators, as well as by the entities covered by these laws. Of note in that regard, ARRA requires both HHS and FTC to report to Congress by February 18, 2010 with recommendations for privacy and security protections for PHRs not covered by HIPAA.

To help build a more comprehensive framework of protections, policymakers at both the federal and state

level might consider the following specific, significant gaps that remain in health information privacy in California despite the combined regulations of HIPAA, ARRA, and CMIA, and steps that could be taken to mitigate those gaps.

Enforcement. Historically, enforcement of HIPAA privacy and security rules has been minimal. Recent changes in both California and federal law create new opportunities for enhanced enforcement, which should include oversight and auditing of the practices of the various entities handling health care information.

Extent of coverage. Neither ARRA-enhanced HIPAA nor CMIA fully protects all health information because certain entities that hold health data fall outside the coverage of both these laws. Privacy and security protections should be extended to data regardless of who created it or now has custody or control over it.

Regulatory guidance. Improved guidance from federal and state regulatory agencies can assist in implementation of protections by covered entities, awareness by patients of their rights and potential violations of them, and enforcement by appropriate authorities of privacy protections. Provisions in ARRA call for several federal rulemakings, and the recently reconstituted CalOHII should provide guidance as needed on implementation of CMIA.

Individual legal redress. California law permits a private right of action for negligent disclosure of personal health information. However, there is no concomitant federal right of action. The ARRA will (within three years) allow individuals to receive a portion of penalties collected during government enforcement actions, but this still leaves them dependent on federal or state authorities to pursue violations. If there were to be a new federal private right of action, it need not be unrestricted: It might permit individuals to enforce the law only in the most egregious cases (such as those involving willful neglect); or it might establish compliance safe harbors for HIPAA-covered entities and their business associates, with individuals permitted to sue only in cases where the entities' behavior exceeded the safe harbor limits.

Marketing restrictions. CMIA and ARRA erect barriers to the unauthorized use of health information for marketing purposes, but both laws still include potentially broad exceptions. Survey data shows a high degree of public concern about the use of personal health information for marketing. To build public trust in the health system's use of information, particularly in the context of increasingly sophisticated information technologies, policymakers could require that any marketing communications intended to facilitate "treatment" or "care management" be sent or authorized by professional caregivers directly involved in an individual's care.

PHR vendors. In ARRA, Congress specifically recognized and at least partially addressed the rapidly expanding area of personal health records offered outside the traditional health care structure. ARRA applies breach notification requirements to PHR vendors and tasks the FTC with enforcing these new requirements. While breach notification is surely a helpful initial step in protecting individuals using PHRs to store and transmit their private health information, lawmakers and regulators need to develop comprehensive privacy and security protections for PHRs. ARRA requires federal agencies to deliver to Congress recommendations on appropriate privacy and security regulations to protect individuals using PHRs.[61]

Conclusion

Recent laws enacted at both the federal and state level have improved the health privacy landscape for patients in California, but work remains to be done, in particular to build public trust in the privacy and security of electronic health records and information transfer. Policymakers should continue to pay attention to this issue, by both filling gaps in the law and adequately enforcing the protections that have already been enacted. It is also crucial for all entities that maintain or transmit health information to establish responsible business practices that reflect and implement the privacy regulations created by federal and state law. A combination of public and private sector efforts can ensure a comprehensive framework of protections that enables health information technology to drive needed improvements in our nation's health care system without sacrificing patient privacy.

About the Author

Deven McGraw, J.D., is Director of the Health Privacy Project at the Center for Democracy & Technology (CDT). Based in Washington, D.C. and San Francisco, CA, CDT is a non-profit, non-partisan public interest organization dedicated to developing and implementing public policies to protect and advance civil liberties and democratic values on the Internet. CDT's Health Privacy Project promotes privacy and security policies and practices that enable the use of health information technology and electronic health information exchange to improve health care.

Ms. McGraw is active in efforts to establish a nationwide health information network. In addition to directing CDT's Health Privacy Project, she served as co-chair of the American Health Information Community's (AHIC) Confidentiality, Privacy and Security Workgroup and was a member of AHIC's Personalized Health Care Workgroup, both of which provided recommendations to AHIC and the Department of Health and Human Services about facilitating greater use of health information technology. She also serves on the Leadership Committee of the eHealth Initiative and co-chairs its privacy and security working group.

About the Foundation

The California HealthCare Foundation is an independent philanthropy committed to improving the way health care is delivered and financed in California. By promoting innovations in care and broader access to information, our goal is to ensure that all Californians can get the care they need, when they need it, at a price they can afford. For more information, visit **www.chcf.org**.

Endnotes

1. Pub. L. 104 – 191, 110 Stat. 1936 (1996) (codified at Title XI of the Social Security Act). Throughout this paper, "HIPAA" is used broadly to refer to requirements found not only in the statute itself but also in HIPAA privacy and security regulations.
2. California Civil Code §§56 – 56.37.
3. Pub. L. 111-5, 123 Stat. 115 (2009).
4. The privacy provisions in ARRA, and the commitment of federal funds for health IT, can be found in the section of ARRA often referred to as HITECH (Health Information Technology).
5. Social Security Act §1178.
6. 45 C.F.R. §160.103; California Civil Code §56.05(f).
7. Social Security Act §1172(a).
8. For HIPAA descriptions of "covered entities," see **www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html**.
9. 45 C.F.R. §§164.502(e) and 164.504(e).
10. California Civil Code §56.05(c). The section defines a contractor as "any person or entity that is a medical group, independent practice association, pharmaceutical benefits manager, or a medical service organization and is not a health care service plan or provider of health care." Notably, it does not include insurance institutions or certain pharmaceutical benefits managers licensed under the Knox-Keene Health Care Service Plan Act.
11. A.B. 1298, amending California Civil Code §56.06(a).
12. 45 C.F.R. §164.506.
13. California Civil Code §§56.10-56.17.
14. 45 C.F.R. §164.502(b).
15. 45 C.F.R. §164.508(a)(3).
16. 45 C.F.R. Part 2; California Health and Safety Code §123105(b).
17. California Health and Safety Code §120975 et seq.
18. 45 C.F.R. §164.508(a)(2); California Civil Code §56.104.
19. 45 C.F.R. §164.528.
20. Id.
21. 45 C.F.R. §164.524; California Health and Safety Code §123100.
22. California Health and Safety Code §123110.
23. Id.
24. See generally 45 C.F.R. §164.501; California Civil Code §§56.05 and 56.10. See also California Civil Code §1798.91.
25. Id.
26. California Civil Code §§56.05(f) and 56.10(d).
27. California Civil Code §§1798.29 and 1798.82.
28. Alonso-Zaldivar, R. "Effectiveness of Medical Privacy Law Is Questioned." *Los Angeles Times,* April 9, 2008.
29. Swire, P. "Justice Department Opinion Undermines Protection of Medical Privacy." *Center for American Progress,* June 7, 2005.
30. California Civil Code §§56.35-36.
31. California Health and Safety Code §1280.15.
32. California Health and Safety Code §§130200 – 130205; see also California Health and Safety Code §1280.15.
33. ARRA §§13401 and 13404.
34. Id.
35. ARRA §13408.
36. Because ARRA did not make all HIPAA privacy and security rules applicable to business associates, accountability will depend on the specific HIPAA regulatory provision at issue and on the terms of the data use or business associate agreement with the covered entity. See Center for Democracy & Technology, "Summary of Health Privacy Provisions in the 2009 Economic Stimulus Legislation," at **www.cdt.org/healthprivacy/20090324_ARRAPrivacy.pdf**.
37. ARRA §13408.
38. ARRA §13405(b).

39. Id.

40. ARRA §13405(a).

41. ARRA §13405(c).

42. 45 C.F.R. §164.524(c)(2).

43. ARRA §13405(e).

44. See ARRA §13401 (an electronic health record is "an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.")

45. ARRA §13406(a).

46. Id.

47. Id.

48. ARRA §13405(d).

49. Id.

50. ARRA §13402; see also §13401 for the definition of "breach."

51. ARRA §13402.

52. ARRA §13407.

53. Id.

54. ARRA §13410(e).

55. ARRA §13410(d).

56. ARRA §13410(f).

57. ARRA §§13401 and 13404.

58. ARRA §13409.

59. ARRA §13410(c).

60. ARRA §13411.

61. ARRA §13424(b).