

## E-Health: Technologic Revolution Meets Regulatory Constraint

*An Internet-driven health system poses new challenges for an area already thick with regulations.*

**by Bruce Merlin Fried, Gadi Weinreich, Gina M. Cavalier, and Kathleen J. Lester**

**EDITOR'S NOTE:** Several burning questions persist in discussions of e-health and its transformation of the U.S. health care system: What is the proper role of government in regulating e-health or keeping its distance? How does e-health fit into existing regulations and governmental health data initiatives? How can the industry act responsibly to smooth its own path toward widespread acceptance? What is the impact on consumers, as more and more health-related transactions take place online, with and without their knowledge? This set of Perspectives was solicited in an effort to provide some answers. The authors represent a variety of views, but all have been active in shaping the roles of government, industry, and consumers. Together the essays cover contiguous territory, joining to fill some of the gaps in this special issue's in-depth examination of the e-health revolution.

**T**HE INFORMATION TECHNOLOGY revolution, exemplified by the expansion of the Internet, promises to shift the U.S. health care system away from the traditional health care delivery model. Profound changes in the business, clinical, and relationship aspects of health care are already occurring. Physicians are no longer the primary source of information for patients. Telemedicine has removed the geographic limits in providing or consulting on clinical care. Web-enabled monitoring devices, linked to online medical records that draw on data warehouses, will permit true

disease management. New models for financing and insuring health care, built on mass customization made possible by health information technology (HIT), are transforming relations among employers, employees, and providers.

This HIT revolution offers both benefits and challenges. Researchers continue to demand validity in critical scientific data. Patients, consumers, and other users of HIT products acutely fear a loss of privacy. Professionals and consumers alike need health information that is reliable. The government, as the dominant health care financier, is insisting that fraud-and-abuse laws be fully applied in e-health transactions.

The e-health revolution is occurring in perhaps our most regulated industry. Congressional and government agency leaders are implementing and proposing a wide array of schemes. In addition, the industry is taking steps toward self-regulation. The challenge is to strike the proper regulatory balance. Heavy-handed regulation will constrain the evolution of the HIT-driven health system, limiting its ability to deliver extraordinary clinical achievements, economic efficiencies, and consumer empowerment. Insufficient regulation will leave the public and physicians—the two groups that ultimately control

---

*Bruce Fried <bruce.fried@shawpittman.com> and Gadi Weinreich are partners in the law firm Shaw Pittman, Washington, D.C. Gina Cavalier is an associate there. Kathleen Lester was with Shaw Pittman at the time of this writing; she is now a privacy consultant for the U.S. Department of Health and Human Services. Fried was director of the Center for Health Plans and Providers at the Health Care Financing Administration and is general counsel to the Internet Healthcare Coalition and the eHealthcare Association.*

health care—dubious about e-health's value.

The e-health industry must navigate this maze of traditional and new regulations before it can realize its potential, in terms of both economics and quality. By examining government and industry initiatives in the new area of content regulation, and the application of established fraud-and-abuse laws to new economies, this paper highlights some of the regulatory challenges and issues facing the e-health industry.

## **Moving Toward Content Regulation**

The e-health industry, as the catalyst for an expansion of health-related information, services, and products, presents new challenges that government regulators, consumers, and the industry itself believe may require new regulatory systems. The need for such regulation stems not only from a desire to protect consumers, as in the case of data privacy initiatives, but also from an understanding that for the benefits of the e-health industry to be maximized, users must trust the system. Demonstrating compliance with a regulatory scheme is one method of establishing such trust. Another method is adoption of industry codes of conduct. The tension between industry self-regulation and direct government regulatory involvement is exemplified by the current debate over regulating content on the Internet.

There are literally millions of health-related pages on the Internet. Information that was once largely physically and intellectually inaccessible to most people is now available online in reader-friendly formats. Through various Web sites, consumers can learn about their health conditions, ask questions of each other and of professionals, track their own health status, search for providers, and volunteer to participate in clinical trials.

The explosion of information raises two content-related concerns. First, patients, providers, and others who are relying on the Internet to gain new choices, knowledge, and opportunities must be able to trust the qual-

ity of the information provided. Second, the vastness of the content increases the chances for misinterpretations and errors or manipulation and deceit. Indeed, ensuring that the content of the Internet is reliable and of high quality, neither misleading nor deceptive, is one of the most crucial barriers the e-health industry must overcome to gain users' trust.

Not surprisingly, as more people look to the Internet for answers to their health questions, advertisers will seek to obtain space on these Web pages. Direct-to-consumer (DTC) advertising on the Internet will likely flourish, especially because by using tracking methods, such as Internet "cookies," advertisers can tailor advertisements to users' preferences. Yet consumers, especially patients, may worry that the tracking methods used to tailor advertisements to them may also be used to track and collect their personal health information. In addition, the increased visibility of advertisements linked to providers may lead users to mistrust information they suspect is tainted by commercial motives.

Today, no overall scheme exists to address these content-related trust issues.<sup>1</sup> The "state of the world" is a mix of efforts at industry self-regulation, First Amendment standards, and a handful of government initiatives. While these ingredients provide a useful base for addressing content-related issues, they will form the appropriate framework only if the various organizations developing and enforcing them, as well as those that are subject to them, work together to create a coherent system that strikes a balance between maintaining the Internet as a "marketplace of ideas" and protecting for consumers who may not understand the source of the information they get from the Internet or what information such sources collect from them.

■ **Industry self-regulation.** Three e-health industry leaders in self-regulation are Health on the Net (HON) Foundation, Health Internet Ethics (Hi-Ethics), and the Internet Healthcare Coalition (IHC).<sup>2</sup> These organizations have developed codes of conduct for e-health content providers to enable these

providers to obtain credibility and Internet users' trust. Each of these organizations has a unique approach; together they address many of the concerns raised regarding the quality and security of Internet content. Enforcement of these principles and codes, however, remains unsettled.

*The HONcode.* The Health on the Net Foundation Code of Conduct (HONcode) for medical and health Web sites represents an international initiative to "standardize the reliability of medical and health information on the World Wide Web" through the adoption of a standard set of principles.<sup>3</sup> HONcode membership is free. Using the HONcode Check tool, an entity must complete a questionnaire to verify that its Web site follows the HONcode principles and identify the changes, if any, that must be made to ensure compliance. A site must then register in the HONcode database. Once this step is completed, HON will e-mail the HTML code for posting the "active seal and logo" on the Web site to the member entity. Only Web sites that adhere to the HONcode may display the active seal and logo. HON promises to monitor the Web site through periodic visits and reviews to ensure compliance.<sup>4</sup>

*Hi-Ethics.* Composed of twenty prominent commercial e-health Web sites, Hi-Ethics has developed ethical guidelines for providing Internet health services to consumers. Its goals are to provide high-quality services that adhere to high ethical standards, ensure that information provided is trustworthy and current, maintain the confidentiality and security of personal information, and enable consumers to distinguish between Internet health services that comport with its standards and those that do not.<sup>5</sup>

In May 2000 Hi-Ethics released fourteen principles with which its members intend to comply by 1 November 2000.<sup>6</sup> In fashioning these principles, Hi-Ethics worked with the leaders of the IHC (see below) to ensure consistency with that organization's code of ethics.<sup>7</sup> Although it remains unclear how Hi-Ethics will enforce these principles, the organization

correctly notes that any Web site claiming to comply with the principles could face sanctions for deceptive trade practices by either the Federal Trade Commission (FTC) or any state attorney general.<sup>8</sup> Hi-Ethics also is attempting to develop industry and government cooperative enforcement mechanisms.<sup>9</sup>

*Internet Healthcare Coalition.* The IHC is a coalition of individuals that seeks to provide users with a high level of confidence in, as well as an understanding of the risks of, using the Internet as a tool to manage their own health and the health of others in their care.<sup>10</sup> In February 2000 the IHC held an e-Health Ethics Summit in Washington, D.C. Conversations from this summit formed the basis for the draft eHealth Code of Ethics. The Hastings Center assisted the IHC Steering Group (composed of ethicists, physicians, and others in the e-health industry) in compiling the draft.<sup>11</sup> In May 2000 the IHC released the final version. The IHC hopes that these principles will serve as a model for self-regulation.<sup>12</sup>

The release of this code marks the achievement of the IHC's first objective.<sup>13</sup> With this task behind it, the organization plans to create an implementation method, which is likely to include the use of a seal on Web sites adhering to the code and revocation of the seal if the Web site fails to follow its principles.<sup>14</sup> In addition, the IHC plans to launch a public education campaign to raise awareness of content issues and provide users with information to make informed choices.<sup>15</sup>

*Remaining questions.* E-health leaders should be applauded and supported in their efforts to craft a code of ethics for their industry although several questions remain unanswered. For example, how effective will the standards be? How widely will they be adopted? Who will ensure compliance? What will happen to Web sites that breach the standards? How will users know to look for these logos or what they indicate? One of the benefits of the Internet is the ability to link to other Web sites for additional content, services, and products. Will it be clear when a user is leaving a code-compliant site and moving into one

controlled by an entity that does not adhere to the industry standard? Should Web sites wishing to adhere to the standards refrain from providing links to sites that do not? Are these standards enough? Do they establish the best practices, or do they merely provide generalized ideals that in reality do not provide enough protection? The answers to these questions are, as yet, unknown. Clearly, however, the industry faces a daunting task.

#### ■ Government initiatives.

The federal government also has begun exploring ways to address concerns over Internet content. The Clinton administration has stressed the need for self-regulation with a limited role for government.<sup>16</sup> Congressional efforts now focus on protecting minors, as do some of the FTC approaches.<sup>17</sup> Some of the government approaches begin to tackle the problems by targeting specific content and enforcing the regulation of e-health Web sites. For example, the FTC seeks to protect consumers from unfair or deceptive practices through its enforcement of the Federal Trade Commission Act (FTCA).<sup>18</sup> These efforts, however, are all checked by the First Amendment.<sup>19</sup>

Congressional attempts to regulate the Internet highlight the difficulty of applying old laws to new technologies. In 1996 Congress passed the Communications Decency Act (CDA) to protect children from "obscene or indecent" material.<sup>20</sup> The Supreme Court struck down some of the statute's provisions, finding them vague and overly broad.<sup>21</sup> In reaching this conclusion, the Court found that the Internet lacked those special factors—history of government regulation, scarcity of frequencies, and the media's invasive nature—that Congress has relied upon to regulate the content of broadcast media. Thus, any regulation of the Internet would fall under the weight of the First Amendment guarantee of free speech unless it could withstand strict scrutiny review. In practice, this

means that a state would have to establish its compelling interest in restricting the Internet usage in question and that the restriction would further some governmental purpose.

Even with this defeat, Congress has enacted, and the FTC has issued regulations pursuant to, the Children's Online Privacy Protection Act (COPPA).<sup>22</sup> This law criminalizes communications for commercial purposes that harm minors unless the entity restricts access to its Web site by requiring a credit card number. A U.S. District Court, however, issued a permanent injunction to keep the Department of Justice (DOJ) from enforcing COPPA, and a U.S. Court of Appeals has upheld this decision.<sup>23</sup> Even though these laws and regulations do not directly implicate all e-

**"It will be difficult to draw the line between scientific disagreement and scam artists preying upon the gullible."**

health Web sites, they demonstrate Congress's desire to regulate Internet content that it finds objectionable.<sup>24</sup>

Although it seems unlikely that Congress will take a direct, content-based approach to regulating e-health Web sites, it could seek to place restrictions on some content under a theory that the speech associated with such sites is "commercial" speech. Although entitled to First Amendment protection, commercial speech is subject to "intermediate scrutiny," rather than the strict scrutiny under which federal courts have evaluated the CDA and COPPA. The use of this lower standard means that the Supreme Court is more likely to find that a restriction does not violate the First Amendment. To be a permissible regulation of commercial speech, a law must meet the four-part *Central Hudson* test: (1) the speech must concern a lawful activity and not be misleading; (2) the government's interest in regulating the speech must be substantial; (3) the regulation must directly advance that interest; and (4) the government's interest would not be met by using a more limited restriction.<sup>25</sup>

Could a regulation restricting the adver-

tisements on a physician's Web page for the sole purpose of protecting consumers from "unwarranted" inferences—that the advertisement implies the physician's endorsement of the advertiser—withstand judicial scrutiny? Along another line, would the Web pages themselves be considered advertisements? If so, could the government place restrictions on the type of medical advice provided through these pages? For example, would regulators be able to prohibit discussions about unpopular methods of treatment? What about alternative medicines? Federal regulations restricting advertisements that are false or misleading clearly withstand judicial review. The issues presented here, however, are much more difficult.

The FTC now focuses its efforts on educating consumers and businesses about illegal practices and how to protect themselves from fraud and deception.<sup>26</sup> The FTCA permits some level of content regulation in that it protects consumers from unfair methods of competition and unfair or deceptive acts or practices affecting commerce.<sup>27</sup> Even though the FTC continues to enforce the act against Internet-based organizations violating its standards, it does not seek additional authority to address content issues directly. The FTC may enforce the FTCA through broad authorization provisions, which include the ability to issue complaints, conduct administrative adjudications, issue cease-and-desist orders, file suit in federal district court for injunctive relief or redress or disgorgement of illegal gains, and file criminal contempt proceedings or criminal actions with the assistance of the DOJ.<sup>28</sup> Most of the Internet cases have involved deceptive advertising, billing practices, and scams (such as pyramid schemes).<sup>29</sup>

Although it appears that the FTC will focus on deceptive practices that harm consumers, in the e-health context it is not clear what "deceptive" means. For example, in addition to obtaining access to Web sites that support the "traditional" medical communities' point of view, patients also will be able to learn

about alternative approaches and theories that some traditional providers might consider misleading or deceptive. As always, it will be difficult for society to draw the line between legitimate scientific disagreement and scam artists preying upon gullible or vulnerable populations. Web sites that post policies stating adherence to industry standards that they do not actually follow or that make misleading or untrue promises or claims risk sanction by the FTC.

Thus, while government initiatives have the potential to regulate e-health content and protect patients and other consumers, current regulation is accomplished only in a roundabout way or as a by-product of traditional proconsumer regulation.

■ **The synergy of self-regulation and government intervention.** Unquestionably, the e-health aspects of the technology revolution present patients, providers, and others with the promise of more knowledge, more opportunities, and more choices regarding their health care decisions. At the same time, the lack of well-established industry brand names synonymous with quality and trust may cause some to avoid using the Internet to its fullest potential. At least at this time, it appears that government views its role as a limited one and primarily will rely upon the industry to police itself. The effectiveness of this approach remains to be seen, as industry leaders emerge and develop enforcement mechanisms to ensure that e-health organizations publicly accept and embrace the evolving industry standards. When coupled with the FTC's enforcement of the FTCA, the emergence of industry standards is likely to create the synergy needed to compel compliance and eventually earn consumers' trust.

### **New Economies Meet Old Laws**

Business arrangements and transactions that are structurally sound from a business perspective frequently implicate (and occasionally violate) the principal federal laws designed to prevent and deter fraud and abuse within Medicare, Medicaid, and other feder-

ally funded health care programs. The application of traditional fraud-and-abuse laws to emerging e-health ventures demonstrates the challenge of trying to fit new arrangements within the parameters of laws that were crafted long before such financial relationships were contemplated. E-health entrepreneurs, often more attuned to e-commerce than to health care, are surprised and perplexed by the limits on their revenue models that result from fraud-and-abuse laws. As a result, at least initially, this type of regulatory constraint may inhibit e-health innovation. The potential tension between emerging e-health ventures and government regulation can be traced to three federal fraud prevention laws: the federal health care program anti-kickback statute, the physician self-referral (“Stark”) law, and the beneficiary inducement law.<sup>30</sup>

■ **Anti-kickback statute.** Under this statute it is illegal to “knowingly and willfully” offer or pay “remuneration”—directly or indirectly, overtly or covertly, in cash or in kind—to “induce” a person to (1) “refer” a person to someone for the furnishing (or arranging for the furnishing) of any item or service for which payment may be made under a federal health care program; (2) “purchase” or “order” any item or service for which payment may be made under a federal health care program; or (3) “arrange for or recommend” purchasing or ordering any item or service for which payment may be made under a federal health care program.<sup>31</sup>

Given the broad application of the anti-kickback statute, e-health ventures must be carefully analyzed and structured, to minimize the potential for program abuse and enforcement risk. Many entities are offering providers “free” Web sites. Whether these offers constitute remuneration designed to induce providers to refer patients to the entity is a threshold question. While the initial development of the Web site may require only a minimal capital outlay on the part of the entity, the government would still likely view the provision and maintenance of a Web site

as “in kind” remuneration—that is, something of value. As Web sites continue to develop and users begin to rely on these resources, the sites will have much greater value, and their free provision would almost certainly qualify as remuneration under the statute.

The next issue is whether “one purpose” of this remuneration is to induce providers to refer patients to the entity. The entity could contend that its primary purpose for providing and maintaining the Web sites is to begin to integrate and streamline certain administrative and business relationships. The expansive scope of the anti-kickback statute is particularly evident here, however, where despite other (legitimate) business reasons for providing the remuneration, regulators could easily argue that “one purpose” was to facilitate referrals; the statute thus would apply.

E-health innovators must struggle to conform new financial arrangements to fit within a very broad statutory and regulatory scheme that never contemplated such structures. At the same time, however, it is important to recognize that Congress has vested the Department of Health and Human Services (HHS) with the authority to protect certain arrangements via regulation. In this way, the anti-kickback prohibition will continue to evolve and may be “updated periodically to reflect changing business practices and technologies in the health care industry.”<sup>32</sup>

■ **Physician self-referral.** The Stark law (named for its sponsor, Rep. Fortney “Pete” Stark, D-CA) prohibits physicians from “referring” Medicare patients to an “entity” for the furnishing of “designated health services” (DHS) if the physician (or an immediate family member) has a “financial relationship” (an ownership or investment interest or a compensation arrangement) with the entity, unless the relationship fits within an exception.<sup>33</sup> The law also prohibits an entity that has provided DHS to an improperly referred patient from submitting a claim (to any person or party) for such DHS.<sup>34</sup> “Referral” is broadly defined under the Stark law. Accordingly, a physician has made a “referral” any

time he or she (1) “requests” DHS or (2) “requests” or establishes a plan of care that includes DHS.<sup>35</sup>

Similar to the anti-kickback statute, any analysis under Stark requires a systematic, critical review of the statutory and regulatory scheme. While it is difficult (although not impossible) to structure many transactions involving physicians to fit within the confines of Stark, proposed regulations could expand the available exceptions and may offer new flexibility for e-health ventures.<sup>36</sup> Further, it is possible that new regulations will be promulgated to cover new economic relationships arising from the technological revolution.

■ **Beneficiary inducement.** This law prohibits a person from offering or transferring “remuneration” to a beneficiary of the Medicare, Medicaid, or other governmental health care program, where such person “knows or should know” that such remuneration is “likely to influence” the beneficiary to order or receive items or services from a particular provider, practitioner, or supplier for which payment may be made (in whole or in part) by Medicare, Medicaid, or another government program.<sup>37</sup>

The beneficiary inducement law could be implicated if, for example, patients could access electronic coupons, from physicians’ Web sites, good for a discount on medications and supplies at a pharmacy that is part of a health system. An analysis of this arrangement depends on such things as whether the coupons were valid only for nonprescription supplies, which are generally not covered by Medicare or Medicaid, or if the coupons were of “nominal value,” an exemption to the remuneration provision.

## Concluding Comments

We stand at the intersection of health care and information technology, and the potential for truly extraordinary health care lies before us. Patients will be empowered with deep knowledge, highly specific personalized health promotion, and self-care strategies and connections to communities of patients, fami-

lies, and providers. Clinicians will be able to immediately access online medical records anytime, anywhere. Disease management systems powered by data warehouses will make evidence-based medicine the norm. Payers, both public and private, will be connected to providers, allowing for rapid and accurate financial transactions and management. Market forces will be brought to bear on an industry that has been remarkably resistant to competition, allowing employers and consumers to make value-based purchases.

Information technology will become faster, more powerful, and cheaper. Scientists, entrepreneurs, and innovators will apply these technologies and their imaginations to the many challenges of the health care system. Society in turn will demand equitable and accessible health care information and service.

Whether any of these realities comes to be will hinge largely on how heavily we regulate e-health. Much about e-health is frightening and has yet to gain our trust. In such situations, societies turn to law and regulation to constrain behavior. The challenge for policymakers, whether from industry or government, will be to strike a balance that fosters innovation and evolution while winning the public’s trust.

## NOTES

1. A related content-based issue is that of liability for libel. For example, several Web sites are considering allowing consumers to rate their providers, with the results published on the site. If a provider believes it has been libeled by a patient, will the host of the site be responsible? As a U.S. Court of Appeals noted, 47 U.S. Code, sec. 230 provides federal immunity from liability for computer service providers who post information originating from a third party. See *Ben Ezra, Weinstein, and Co. v America Online, Inc.*, 206 F.3d 980, 984–985 (10th Cir. 2000).
2. Another prominent industry leader is TRUSTe, <[www.truste.com](http://www.truste.com)>. Because its principles primarily address confidentiality concerns, it is beyond the scope of our discussion.
3. See “Principles,” *HON Code of Conduct for Medical and Health Web Sites*, 25 January 2000, <[www.hon.ch/Conduct.html](http://www.hon.ch/Conduct.html)> (12 August 2000).
4. *Ibid.*, “HONcode Membership Application” (4 July 2000), <[www.hon.ch/HONcode/HONcode\\_](http://www.hon.ch/HONcode/HONcode_)

- membership.html> (12 August 2000).
5. See *Health Internet Ethics: Ethical Principles for Offering Internet Health Services to Consumers*, <[www.hiethics.org/Principles/index.asp](http://www.hiethics.org/Principles/index.asp)> (12 August 2000).
  6. *Ibid.*
  7. *Ibid.*
  8. See <[www.hiethics.org/FAQ.asp](http://www.hiethics.org/FAQ.asp)> (12 August 2000).
  9. *Ibid.*
  10. See "Mission Statement," <[www.ihealthcoalition.org/about/mission.html](http://www.ihealthcoalition.org/about/mission.html)> (12 August 2000).
  11. See *eHealth Code of Ethics*, <[www.ihealthcoalition.org/ethics/ehcode.html](http://www.ihealthcoalition.org/ethics/ehcode.html)> (12 August 2000).
  12. *Ibid.*
  13. Helga Rippen, director of medical informatics, Pfizer Health Solutions, and IHC steering group member, public remarks delivered 24 May 2000, Washington, D.C., upon release of the code.
  14. *Ibid.*
  15. *Ibid.*
  16. The White House, *The Framework for Global Electronic Commerce*, 1 July 1997, <[www.whitehouse.gov/WH/New/Commerce/read.html](http://www.whitehouse.gov/WH/New/Commerce/read.html)> (12 August 2000).
  17. The two most prominent congressional efforts in the past few years are the Communications Decency Act (CDA), 47 U.S. Code, sec. 223, and the Children's Online Privacy Protection Act (COPPA), 47 U.S. Code, sec. 231. For FTC approaches, see 64 *Federal Register* 59888 (1999).
  18. Robert Pitofsky, chairman, Federal Trade Commission, testimony before the Senate Governmental Affairs Subcommittee on Investigations (10 February 1998).
  19. See *Reno v ACLU*, 521 U.S. 844 (1997) (defining the Internet as a form of communication with so few barriers that the Court will review restrictions upon it with strict scrutiny).
  20. 47 U.S. Code, sec. 223.
  21. *Reno v ACLU*, 844.
  22. 47 U.S. Code, sec. 231; and 64 *Federal Register* 59888.
  23. *ACLU v Reno*, 217 F.3d 162 (3d Cir. 2000).
  24. E-health entities may find themselves the targets of such initiatives as they venture into providing health services that some could view as obscene. It is easy to imagine a mental health Web site that provides a chat room for teens dealing with depression in which the teens frankly discuss topics that others might view as indecent. If so, these laws raise concerns for such Web sites.
  25. This test is derived from the Supreme Court's decision in *Central Hudson Gas v Public Service Commission*, 447 U.S. 557, 566 (1980), in which the Court invalidated a prohibition on advertisements by utility companies that promoted the use of electricity. Although the First Amendment commercial speech doctrine has been churning, the Court continues to rely upon the *Central Hudson* test as a benchmark for its analysis. See 44 *Liquormart, Inc. v Rhode Island*, 116 S.Ct. 1495 (1996). For a more detailed explanation of the fluctuating doctrine, see K.J. Lester, "Cowboys, Camels, and Commercial Speech: Is the Tobacco Industry's Commodification of Childhood Protected by the First Amendment?" *Northern Kentucky Law Review* 24 (1997): 615, 642-648.
  26. Pitofsky, testimony.
  27. 15 U.S. Code, sec. 45(a).
  28. *Ibid.*, secs. 45(a), 53(b), and 56.
  29. See, for example, FTC File no. 952-3331, 1 May 1997 (settling allegations that "free trial" offers resulted in unexpected charges for many consumers), <[www.ftc.gov/os/1997/9705/ameronli.htm](http://www.ftc.gov/os/1997/9705/ameronli.htm)> (25 August 2000); and *FTC v The Mentor Network, Inc.*, FTC File no. X970015, 17 March 1997 (consent decree requiring defendants to pay \$75,000 into a fund for consumer redress and barring defendants from operating any chain or pyramid marketing program), <[www.ftc.gov/os/1997/9703/mentor.htm](http://www.ftc.gov/os/1997/9703/mentor.htm)> (25 August 2000).
  30. These laws and their regulations are exceptionally complex. It was not possible to fully explore these policies in the space available. The authors encourage e-health entities to seek advice from competent health care counsel in developing their business plans and revenue models.
  31. 42 U.S. Code, sec. 1320a-7b(b)(2). It also is illegal to "solicit" or "receive" remuneration for such purposes. *Ibid.*, sec. 1320a-7b(b)(1). Many states have their own counterparts, some of which are even broader than federal law.
  32. 64 *Federal Register* 63517 (1999).
  33. Designated health services include laboratory, therapy, and radiology services; durable medical equipment; prosthetics and orthotics; home health services; outpatient prescription drugs; and inpatient and outpatient hospital services. 42 U.S. Code, sec. 1395nn(h)(6).
  34. *Ibid.*, sec. 1395nn(a)(1)(B).
  35. *Ibid.*, sec. 1395nn(h)(5)(A)-(B).
  36. 63 *Federal Register* 1659 (1998). We expect the final version of these regulations to be published shortly.
  37. 42 U.S. Code, sec. 1320a-7a(a)(5).