Education and debate

Regulating health information: a US perspective

Nicolas Terry

Technologically mediated health care raises problems of quality of information, cross border practice, and patient confidentiality. Nicolas Terry probes the legal aspects of these complexities, and Benedict Stanberry adds a European perspective

Center for Health Law Studies, Saint Louis University School of Law, 3700 Lindell Blvd, St Louis, MO 63108, USA

Nicolas Terry
professor

terry@slu.edu

BMJ 2002;324:602–6

Identifying the regulatory agenda for health information is not difficult. The quality of publicly available health information, cross border medical and pharmacy practice, and the privacy of medical records appear on the radar screens of most public health and consumer protection organisations. Left unregulated, any of these issues can cause considerable harm. Each issue also embodies difficult tensions: state versus federal rights, increased access to care versus quality assurance, and confidentiality versus professional discourse.

US state and federal legal systems have not achieved a coherent approach to regulating the dissemination of health information. Furthermore, the American experience will not always transfer directly to publicly funded medicine and government initiatives. Nevertheless the American experience with private sector ehealth is an instructive model, even if some areas have been neglected and others over-regulated.

Summary points

- Quality of publicly available health information, cross border medical and pharmacy practice, and privacy of records will be key issues for European regulators
- Concerns about medical advice sites may be exaggerated
- US regulators have yet to find the appropriate balance between risk and benefits of cross border practice
- New US federal laws on health privacy appear cumbersome but may be instructive for other legal systems

Regulating the quality of online health information

Concerns about widespread inaccuracies in online health information are speculative and intuitive rather than based on robust research. Berland's quality assessments, at least for English language sites and well educated users, suggest the picture is not so gloomy as critics expected.[1]

Public law regulation of health information may conflict with US guarantees of free speech, and differences of opinion among medical professionals make the broad regulation of health advice difficult. Consequently, intervention through public law is reserved for obviously dangerous health content where government agencies can apply traditional consumer protection, drug regulation, and fraud powers, as with the Federal Trade Commission's "Operation Cure.All."[2]

Arguments about freedom of speech can be used to defend private legal actions against web sites offering medical advice, and precedents from actions against publishers of "advice" or "how to" books show that such claims are hard to win.[3] Case by case, retrospective, private law "regulation" may, however, be judicially more acceptable than blanket public law regulation.

Since regulation can do only so much to deter the web's snake oil salesmen, the focus inevitably shifts to strengthening the role of the market by reducing the costs of health information to the consumer. "Kitemark" or "trustmark" schemes seek to limit the need for consumers to assess the quality of information themselves by encouraging providers to rate their own contributions or to comply with codes of conduct. With compliance or rating in place, a technology layer can be added that leverages downstream filtering technology or upstream filtering through membership in a distinct top-level domain[4]; Medcertain is an example of downstream filtering technology,[5] whereas the World Health Organization

favours the upstream approach.[6] Filtering persuades content producers to participate in ratings systems because search engines and, increasingly, browsers may be set to ignore unrated sites.

One approach that is emerging in the United States is to combine the evaluation of online content—for example, kitemarking—with private accreditation, a quality assurance system widely adopted by bricks and mortar healthcare providers.[7] For this, a provider of online health information would subscribe to an accrediting agency's quality standards and pay the agency to check for compliance. Accreditation is a particularly interesting model because it uses a well respected method of quality assurance that is already recognised in private malpractice actions and brings traditional healthcare bodies and online providers under the same quality assessment umbrella. The use of such a model will also be of interest to litigators as US courts have held that failure to comply with applicable accreditation standards may constitute sufficient evidence of medical malpractice.

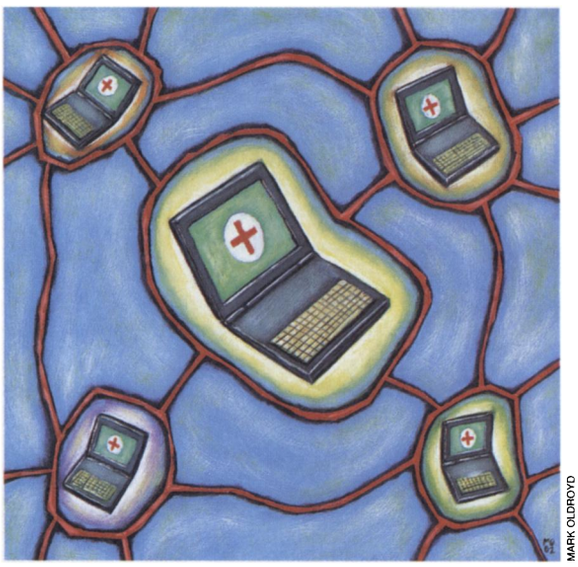
Whether simple or sophisticated, and whether relying on self regulation or rating by third parties, kitemarking systems are not without their difficulties,[8] critics,[9] or legal pitfalls, including the potential liability of rating organisations to private legal actions.[10] The voluntary adoption of codes of conduct in good faith by health websites should not be trivialised or discouraged. Equally, the potential for fraudulent self rating and the likelihood that kitemarking will reduce consumers' natural skepticism about health information continue to trouble US regulators; this may explain a lack of enthusiasm relative to that of their colleagues in Europe.

Controlling cross border practice

With the appearance of online medical advice sites, it is easy to overlook the proportion of cross border health information provided by physicians and pharmacists. In the United States, healthcare institutions are subject to national accreditation standards, and they educate their medical students according to a national curriculum with a view toward national testing. Medical professionals, however, are exclusively regulated by state authorities. Most state licensing and disciplinary systems assume that there will be some level of cross border medical practice by providers who consult with colleagues in other states or treat their travelling patients; these activities are not required to be licensed. Such exceptions aside, however, US states insist on local licensing.

Theoretically, increasing cross border services through technologically mediated health care should stimulate interest in an overall liberalisation of cross border practice. In reality, state authorities are strengthening their legislation to deter interstate ehealth services that either originate from or are received within their borders.[11] While some of the voices raised against ehealth may have protectionist accents, the reality is that states' disciplinary and quality assurance powers are tied to the licensing process and there is no political will for moving such functions to a federal body.

In the United States federal regulators have legal competence over drug approval and marketing.



MARK OLDROYD

Nevertheless, pharmacists, like doctors, face a state-by-state system of licensure and discipline. Licensing and quality issues, however, are not such a problem in pharmacy because it is easier for pharmacy chains to comply with multiple licensing requirements. The National Association of Boards of Pharmacy has facilitated compliance and consumer education by setting up a national system for trustmarking online pharmacies.[12] Additional state by state regulation of pharmacists may, however, be imminent. At least one state now believes it can achieve indirectly what it has failed to do directly: stopping internet doctors from writing prescriptions for its citizens by placing the responsibility on the pharmacist to make sure that the prescription was the product of a traditional doctor-patient interaction.[13] Such regulations will function as an indirect but effective method of controlling cross border medical practice.

This stringent regulation of ehealth exchanges across borders assumes too readily that indirect health care is inferior. Valid questions have been raised about the quality of email communications between doctor and patient,[14] particularly doctors' responses to unsolicited email from patients. Though they pose some marginally interesting legal questions, these are essentially transitional issues that call for better education of doctors more than for regulatory intervention. A more important issue is whether doctors must disclose the risks of remote consultations. The American Medical Informatics Association has cogently argued that an informed consent instrument should "provide instructions for when and how to escalate the contact from being via the internet to phone calls and office visits" and that it should "describe the security mechanisms that are in place."[15] Some US states already require specific consent for remote, technologically mediated care and professional organisations increasingly are recommending the use of encrypted systems for doctor-patient communications.[16] Such regulation is appropriate when motivated by concerns over quality or patient autonomy but less so if designed to discourage non-traditional care.

It may be time to review the marketing activities of pharmaceutical companies both on the internet and in more traditional media. Direct to the consumer adver-

tising is commonplace in the United States. The Federal Drug Agency's Center for Drug Evaluation and Research seeks valiantly to enforce advertising standards[17] through its general regulatory standards and processes.[18] In comparison with the constant barrage of pharmaceutical advertising aimed at US consumers, however, regulatory efforts tend to pale into insignificance. Against the background of the tightly controlled environment of doctors and patients under managed care, pharmaceutical companies are using direct to consumer advertising to try and persuade patients to pay for items not covered by their managed care plans, while simultaneously using both patients and doctors to coerce managers of health plans to add the company's products to their formularies. The importance to pharmaceutical manufacturers of direct advertising to consumers, however, may be illustrated by manufacturers' sanguine acceptance of increased exposure to liability for their products when they circumvent the traditional channel—doctor to patient—for drug information.[19]

Apart from suggesting the need for increased direct regulation (such as the American Medical Assoociation's demand that direct to consumer advertising should contain warnings that a doctor might actually recommend a different treatment[20]), the growth of direct advertising presents difficult issues of ethical and possibly legal conflicts of interest for health advice sites that seek click-stream revenue from their links to the sites of pharmaceutical manufacturers or pharmacies.[21]

Privacy of medical information

Health websites on both sides of the Atlantic have failed to establish acceptable standards of data protection.[22] Somewhat ironically, the European Union's green paper exploring the development of a community-wide approach to consumer protection was published within days of the Federal Trade Commission's announcement that it was abandoning plans to introduce any new online privacy legislation.[23] Without such legislation, the commission's ability to protect consumer privacy on the internet is limited to cases where websites breach their own published privacy policies.[24] Websites need not have privacy policies, however, and if they do, the content goes unregulated. The United States' trading partners are justifiably concerned by this neglect for consumer privacy, and the Federal Trade Commission's recent backtracking on guarantees for online privacy for children will increase discomfort.[25]

Although US regulators have been derelict in protecting the general privacy of citizens, concerns regarding the privacy of health information in the United States are not necessarily warranted. The new federal standards for privacy of individually identifiable health information[26] (and related draft security regulations) issued under the Health Information Portability and Accountability Act (HIPAA) provide the world's most robust protection for medical information, although recent developments in Australia threaten that status.[27]

Most modern privacy regimes, including the EU data protection directive,[28] are collection-centric. That is, they limit the collection of consumer information, frequently by reference to a concept such as proportionality. Serious questions arise, however, as to whether health privacy regimes should place any limits on the collection of patient data, at least for purposes related to treatment. Thus HIPPA is a disclosure-centric confidentiality scheme. It protects patient information by prohibiting most disclosures unless they are preceded by highly regulated processes of consent for treatment or payment purposes. Even more stringent provisions, together with a "minimum necessary" rule, limit disclosures for other purposes, such as marketing or fundraising.

These privacy and security rules were not developed in a vacuum. US regulators are introducing a vastly more efficient system for health transactions, based on electronic data interchange. Unfortunately, this origin exposes the fundamental flaw in the HIPAA privacy and security schemes: they apply only to healthcare entities that use the electronic data interchange system. As a result, hospitals, doctors, and health insurers are likely to find their internet activities regulated, while the more typical ecommerce sites offering health advice or medical products, which collect and resell customer information, are far less likely to fall within the regulatory scope. State statutory and common law systems that provide higher levels of privacy protection are not, however, pre-empted by the federal HIPAA scheme. These unharmonised state law protections will become increasingly important as health websites sell their visitor data to research companies[29] and if healthcare organisations continue their unfortunate accidental postings of confidential patient information on the web.[30]

Conclusion

Industry consolidation around a few well known brands and the dot.com implosion have taken their toll on health advice sites. In the near term the major ehealth players will be drawn from basic health organisations looking to technology to improve the quality and efficiency of their services[31] and government agencies seeking to improve healthcare delivery to underserved populations.

It is both appropriate and practical to shift regulatory emphasis away from advice sites. Outdated, inaccurate, fraudulent, or even dangerous information on the web is notoriously difficult to regulate. Our regulatory energies are better devoted to pressing health information problems that are soluble, such as Balkanised approaches to regulating cross border health interactions and the security and privacy of personal medical information.

Competing interests: None declared.

1 Berland GK, Elliott MN, Morales LS, Algarzy JI, Kravitz RL, Broder MS, et al. Health information on the internet: accessibility, quality, and readability in English and Spanish. *JAMA* 2001;285:2612-21.
2 Federal Trade Commission. "Operation Cure.All" wages new battle in ongoing war against internet health fraud. Press release, 14 June 2001. www.ftc.gov/opa/2001/06/cureall.htm (accessed 24 Jan 2002).
3 Terry NP. Cyber-malpractice: legal exposure for cybermedicine. *Am J Law Med* 1999;25:349-58.
4 Eysenbach G. An ontology of quality initiatives and a model for decentralized, collaborative quality management on the (semantic) world wide web. *J Med Internet Res* 2001;3(4):e34.
5 MedCertain. www.medcertain.org (accessed 24 Jan 2002).
6 WHO proposal would raise quality of internet health information. Press Release WHO/72,13 November 2000. www.who.int/inf-pr-2000/en/pr2000-72.html (accessed 24 Jan 2002).

7 URAC, American Accreditation Health Care Commission. Health web site accreditation. www.urac.org/v1-0.PDF (accessed 25 Jan 2002).
8 Jadad AR, Gagliardi A. Rating health information on the internet: navigating to knowledge or to Babel? *JAMA* 1998;279:611-4.
9 Delamothe T. Quality of websites: kitemarking the west wind, *BMJ* 2000;321:843-4..
10 Terry NP. Rating the "raters": legal exposure of trustmark authorities in the context of consumer health informatics. *J Med Internet Res* 2000;2(3):e18.
11 West Virginia Code. W Va Code §30-3-13 (2001).
12 National Association of Boards of Pharmacy. VIPPS. www.nabp.net/vipps/intro.asp (accessed 24 Jan 2002).
13 Texas Administrative Code, 22 Tex. Admin. Code §§291.34, 291.36.
14 Eysenbach G, Diepgen TL. Responses to unsolicited patient email requests for medical advice on the world wide web. *JAMA* 2998;280:1333-5.
15 Kane B, Sands DZ. Guidelines for the clinical use of electronic mail with patients. *J Am Med Inform Assoc* 1998;5:104.
16 Medem. Online medical liability addressed by national consortium: medical liability moves online. Press release, 29 Jan 2002. www.medem.com/corporate/xl_corporate_medeminthenews_detail.cfm?ExtranetPressNewsKey=121 (accessed 25 Feb 2002).
17 Center for Drug Evaluation and Research. Guidance for industry; consumer-directed broadcast advertisements, August 1999. www.fda.gov/cder/guidance/1804fnl.htm (accessed 24 Jan 2002).
18 Center for Drug Evaluation and Research. Warning letters and notice of violation letters to pharmaceutical companies. www.fda.gov/cder/warn/index.htm (accessed 24 Jan 2002).
19 Perez v Wyeth Laboratories Inc. 734 A.2d 1245 (NJ 1999).
20 American Medical Association. House of Delegates, June 19 2001, Resolution 503. www.ama-assn.org/ama/pub/category/4940.html (accessed 24 Jan 2002).
21 Terry NP. AMA Ethics Forum: Making a health web site ethically sound. *Am Med News* 2001 June 4.
22 Consumers International. Privacy@net: an international comparative study of consumer privacy on the internet. January 2001:5-7. www.consumersinternational.org/news/pressreleases/fprivreport.pdf (accessed 25 Jan 2002).
23 Federal Trade Commission. FTC chairman announces aggressive, pro-consumer privacy agenda. Press release, 4 Oct 2001. www.ftc.gov/opa/2001/10/privacy.htm (accessed 24 Jan 2002).
24 Federal Trade Commission. Eli Lilly settles FTC charges concerning security breach. Press release, 18 Jan 2002. www.ftc.gov/opa/2002/01/elililly.htm (accessed 25 Feb 2002).
25 Federal Trade Commission. FTC seeks comment on amending children's internet privacy rule. Press release, 26 Oct 2001. www.ftc.gov/opa/2001/10/slidingscale.htm (accessed 24 Jan 2002).
26 Department of Health and Human Services. Standards for privacy of individually identifiable health information. 65 Fed. Reg. 82462 (28 Dec 2000), http://aspe.hhs.gov/admnsimp/final/PvcTxt01.htm (accessed 24 Jan 2002).
27 Office of the Federal Privacy Commissioner. Guidelines on privacy in the private health sector (October 2001). www.privacy.gov.au/publications/hg_01.html (accessed 24 Jan 2002).
28 Council of the European Communities. Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the member states concerning liability for defective products. http://europa.eu.int/eur-lex/en/lif/dat/1985/en_385L0374.html (accessed 24 Jan 2002).
29 Quintiles and WebMD announce settlement agreement, October 12, 2001. www.quintiles.com/corporate_info/press_releases/press_release/1,1167,891,00.html (accessed 24 Jan 2002).
30 Web mishap: kids' psychological files posted. *LA Times* 2001 Nov 7. www.latimes.com/technology/la-000088956nov07.story (accessed 24 Jan 2002).
31 Terry NP. An eHealth diptych: the impact of privacy regulation on medical error and malpractice litigation. *Am J Law Med* 2001;27:361-419. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=286778 (accessed 7 Feb 2002).

(Accepted 21 January 2002)