Comparing eHealth Privacy Initiatives

November 2001

Prepared for the

California HealthCare Foundation

by

Angela Choy and Janlori Goldman

Health Privacy Project

Institute for Health Care Research and Policy

Georgetown University

Acknowledgments

HEALTH PRIVACY PROJECT
INSTITUTE FOR HEALTH CARE RESEARCH AND POLICY GEORGETOWN UNIVERSITY

The Health Privacy Project is part of the Institute for Health Care Research and Policy at the Georgetown University Medical Center. The project is dedicated to raising public awareness of the importance of ensuring health privacy in order to improve health care access and quality, both on an individual and a community level. For more information, visit www.healthprivacy.org.

The **CALIFORNIA HEALTHCARE FOUNDATION**, a private philanthropy based in Oakland, California, focuses on critical issues confronting a changing health care marketplace by supporting innovative research, developing model programs, and initiating meaningful policy recommendations. For more information visit www.chcf.org.

The iHealth Reports series focuses on emerging technology trends and developments and related policy and regulatory issues.

Additional copies of this report and other publications in the iHealth series can be obtained by calling the California HealthCare Foundation's publications line at 1-888-430-2423 or visiting us online at www.chcf.org.

California HealthCare Foundation
476 Ninth Street
Oakland, CA 94607
tel: (510) 238-1040
fax: (510) 238-1388
www.chcf.org

Key Findings

- Many in the eHealth private sector have established core principles for health Web sites to adhere to in protecting consumer privacy and autonomy. In fact, many of these initiatives have adapted the Federal Trade Commission's (FTC) Code of Fair Information Practice Principles in developing standards and guidelines for protecting the privacy of online health information.

- The self-regulatory efforts differ in focus and comprehensiveness; some offer general principles while others provide detailed rules and examples to assist sites in implementing the standards.

- Because there is a range of self-regulatory standards and programs available to health Web sites, consumers may find it difficult to determine the distinguishing features of each program and may be confused by the various symbols and seals that appear on different sites.

- A key weakness of these self-regulatory efforts is that compliance with online standards is voluntary and there are few, if any, enforcement mechanisms in place for noncompliance.

Overview

Increasingly, consumers are worried about their loss of privacy, especially with regard to personal health information. They are concerned that their information may be used or disclosed inappropriately, leaving them vulnerable to unwanted exposure, stigma, and discrimination. These fears exist whether they engage in health-related activities online or offline. According to a survey released by the Pew Internet and American Life Project in November 2000, 80 percent of "health seekers" say it is important to them that they are able to obtain information anonymously. For the most part, users do not share personal information at health Web sites: only 21 percent have provided their email address; only 17 percent have provided their name or other identifying information; and only 9 percent have participated in an online support group about a health condition. These results are consistent with the findings of an earlier study released by the California HealthCare Foundation (CHCF) of consumers in more traditional health care settings. The 1999 CHCF survey found that almost one in six U.S. adults withdraws from full participation in his or her own health care to keep personal medical information confidential. While many people continue to use the Internet to get health information, they would like to see rules in place to protect their privacy (Markle Foundation survey, July 2001).

A few companies, such as Intel, AOL-Time Warner, and the American Electronics Association (a trade association), acknowledge that privacy is a problem that requires some federal action. Many Internet service providers and online companies, however, such as Earthlink, IBM, and Amazon.com, do not believe federal Internet privacy legislation is warranted, although they would accept limited legislation that preempts state laws and sets a federal standard.

To avoid overzealous federal regulation, while responding to the public's desire for privacy protections online, initiatives have been developed or are underway by the private sector to establish privacy guidelines and standards for health Web sites that incorporate fair information practice principles. While the goal of these initiatives is to promote consumer trust and confidence in health Web sites, many of the standards are only voluntary efforts at self-policing with no penalties and few, if any, enforcement mechanisms for noncompliance. In addition, Hewlitt-Packard Co. had testified before the Senate Commerce Committee in October 2000 that "even with all these self-regulatory efforts..., it is unlikely that the majority of commercial Web sites will post consumer-friendly, easily-readable privacy policies, or join privacy programs, at least in the short run."

With so many guidelines and recommendations available, consumers may find it difficult to determine the distinguishing features of each privacy initiative. For example, Hi-Ethics and TRUSTe have partnered to develop an eHealth Seal program. Hi-Ethics has also partnered with URAC on accreditation standards for health Web sites.

How will the two programs fit together? Will Web sites be required to meet the criteria of both programs? Moreover, will there be efforts to reconcile the differences in terminology for the various standards?

Despite the potential confusion among consumers, it does appear that many of the self-regulatory efforts have adapted the FTC's Code of Fair Information Practice Principles in developing their own guidelines and recommendations. (The principles include: notice, access, choice/consent, security, and enforcement.) A California HealthCare Foundation report, co-authored by the Health Privacy Project, which documented the weaknesses in the privacy policies and practices of 21 major health Web sites, has also become an ongoing framework for privacy policies. Many of the current self-regulatory initiatives include standards for ensuring privacy on health Web sites that address issues of notice, user control and consent, user access to personal information provided to Web sites, security, limits on disclosures, and transparency. While earlier efforts, such as HONcode, offered only general principles for health Web sites; recent initiatives, like URAC's accreditation program and the American Health Information Management Association's (AHIMA) recommendations, provide more comprehensive standards and greater guidance for self-regulation.

Methodology

The accompanying tables summarize the various initiatives and the status of their development and implementation. Comparisons of the self-regulatory initiatives were made against a set of criteria based on the FTC Fair Information Practice Principles—key elements that should be addressed in any privacy standard.

Table 1 compares the self-regulatory efforts that have been or are in the process of being developed by trade associations for use by any health-related Web site. These trade associations were established specifically to address issues of privacy, security, and quality on health sites. Table 2 compares the guidelines and requirements established by professional organizations predominantly for their members who have expanded their offline health care activities onto the Internet. Recommendations from professional organizations generally are derived from traditional health care practice principles and codes of ethics. Guidelines or seal programs that are not specifically designed for health Web sites are not included in these tables.

Table 1. Comparison of Self-regulatory Efforts by Trade Associations

	Hi-Ethics	TRUSTe and Hi-Ethics	URAC and Hi-Ethics	Internet Healthcare Coalition – eHealth Ethics Initiative	Health on the Net (HON) Foundation	eHealth Initiative (eHI)
1. Type of Initiative	Principles: "Ethical Principles for Offering Internet Health Services to Consumers" Coalition of Internet health sites and service providers; some members of Hi-Ethics include America Online, drkoop.com, Medscape, PersonalMD, and WebMD.	Partnership to develop health seal for health Web sites.	Accreditation program for health Web sites: Health Web Site Standards Version 1.0 URAC developed detailed standards based on the 14 Hi-Ethics Principles.	Code of ethics: "eHealth Code of Ethics"	Code of conduct for medical and health Web sites (HONcode); accredits health-related Web sites—self-regulatory, voluntary certification system based on a seal concept.	A national not-for-profit advocacy and trade organization, an alliance of 53 healthcare institutions; its mission is to promote the adoption of the Internet and other emerging technologies to modernize health care delivery. They have not and do not intend to offer recommendations now.
2. Status	Principles released in June 2000. Founding members were expected to implement the principles within six months—by December 2000. Hi-Ethics is currently updating its principles with plans to release version 2.0 of the principles by December 2002.	TRUSTe already has a privacy seal program with almost 2000 members. The partnership with Hi-Ethics is to develop eHealth seals for health Web sites. The end of the third quarter of 2001 is the target date for issuance of the first group of seals.	Accreditation standards for health sites were released on July 30, 2001. Implementation of the standards was expected to begin in August. URAC plans to work with TRUSTe to implement the program.	IHC held an eHealth Ethics Summit to develop a code of ethics. The code was developed by Hastings Center and Summit Steering Group after the Summit and released in May 2000. Organizations endorsing the code include American College of Preventive Medicine, Coalition for Health Information Policy, drkoop.com, MedicaLogic/Medscape, and URAC.	Health on the Net Foundation is a nonprofit, international Swiss organization created in 1995. More than 2,800 sites adhere to the HONcode.	Incorporated on March 19, 2001. Members include IBM, Medscape, Medstar, WellMed, Pricewaterhouse-Coopers, the Internet Healthcare Coalition, and RnetHealth. The organization is working on position statements on specific eHealth issues.

Table 1. Comparison of Self-regulatory Efforts by Trade Associations (continued)

	Hi-Ethics	TRUSTe and Hi-Ethics	URAC and Hi-Ethics	Internet Healthcare Coalition – eHealth Ethics Initiative	Health on the Net (HON) Foundation	eHealth Initiative (eHI)
3. Process	Members of Hi-Ethics agree to adopt the ethical principles and pay a $20,000 annual membership fee. In June 2001, the membership fees were reduced by 70% to $1,500 per quarter. The organization also must be willing to participate in the eHealth Seal program administered by TRUSTe. Now that the URAC accreditation standards have been released, Hi-Ethics will be relying on URAC to verify a site's adherence to the Hi-Ethics principles.	The eHealth seal will be available for Internet companies that meet Hi-Ethics' 14 standard principles of privacy and professionalism (see summary of Hi-Ethics Principles). Pricewaterhouse-Coopers is expected to perform audits to ensure compliance with the principles.	URAC will conduct annual reviews of each site that it accredits to verify continuing compliance. URAC will investigate complaints. Sites that violate the standards will be required to take corrective action or withdraw from the program. There will be a $5,000 application fee.	Compliance with the Code is voluntary.	Web sites apply for registration. A HON team member inspects the site to make sure that all of the principles are followed. If accepted, a site is issued a unique ID number. Compliant sites display the HONcode seal. The sites are responsible for complying with the HON principles.	Members pay annual dues of $2,500 to $25,000. eHI lobbies Congress. It engages in advocacy, education, and other informational activities to address barriers to "realizing the promise of eHealth," including privacy and security.

Table 1. Comparison of Self-regulatory Efforts by Trade Associations (continued)

	Hi-Ethics	TRUSTe and Hi-Ethics	URAC and Hi-Ethics	Internet Healthcare Coalition – eHealth Ethics Initiative	Health on the Net (HON) Foundation	eHealth Initiative (eHI)
4. Notice	Members must adopt privacy policies that are easy for consumers to find, read, and understand and provide users with reasonable notice of the member's information practices, including disclosure of: collection or use of any information about the user; collection or use of aggregate data; and what, if any, access to personal information the site provides to unrelated third parties. Member sites are also required to give notice to users of any changes to its privacy policies.	See Hi-Ethics principles.	Accredited Web sites must prominently post the notice of all disclosures. They are also required to disclose to users (1) what information about them is collected and how it is used, (2) to whom the information may be disclosed, (3) for what purpose, (4) how long the information will be retained, (5) what rights the user has with respect to their personally identifiable information, (6) the entity that maintains their information, and (7) limitations on deletion or removal of that information. If the site uses "passive tracking mechanisms," (e.g., cookies and Web bugs), the site must disclose the use of such mechanisms and the purpose for which they are used, obtain opt-in from users before using such mechanisms, provide means for subsequent opt-out if users previously agreed to tracking, and inform users of consequences of not agreeing to passive tracking.	Sites that endorse the Code should clearly disclose: that there are potential risks to user privacy on the Internet; what data are being collected when users visit the site; who is collecting the data; how the site will use the data; whether the site knowingly shares data with others; and with which organizations or individuals the site shares data and how it expects its affiliates to use that data. The site also must tell users how the site stores the user's personal data and for how long.	HONcode is silent on the issue of notice.	Not applicable.

Table 1. Comparison of Self-regulatory Efforts by Trade Associations (continued)

	Hi-Ethics	TRUSTe and Hi-Ethics	URAC and Hi-Ethics	Internet Healthcare Coalition – eHealth Ethics Initiative	Health on the Net (HON) Foundation	eHealth Initiative (eHI)
5. Choice/ Consent	Users are given "meaningful" choice to accept or decline the site's collection and use of personal information provided by the user, including consent to transfer information to third parties. If a site collects health-related personal information, the site will use it only as agreed to by the consumer or for purposes for which a reasonable consumer would expect the site to use that information. The site will not disclose health-related personal information to unrelated third parties or for unrelated purposes without consent of consumer (via opt-in procedure). If significant changes are made to the privacy policy that affects the use of health-related personal information collected prior to the change, the site will not make use of the information without first obtaining the consumer's consent.	See Hi-Ethics principles.	A site can collect personal health information only for users who opt in and the site must describe the consequences for providing and not providing the information. The opt-in must be obtained from users prior to the collection and use of personal health information. The site must allow users, at any point, to opt-out of the continued collection and use of their information and/or request deletion of that information.	Sites should not collect, use or share personal data without a user's specific affirmative consent.	HONcode is silent on the issue of consent.	Not applicable

Table 1. Comparison of Self-regulatory Efforts by Trade Associations (continued)

	Hi-Ethics	TRUSTe and Hi-Ethics	URAC and Hi-Ethics	Internet Healthcare Coalition – eHealth Ethics Initiative	Health on the Net (HON) Foundation	eHealth Initiative (eHI)
6. Transparency	Member sites with relationships with third parties must adopt procedures to inform consumers whether third parties have access to their information from the site. The sites also must disclose information about site ownership, and financial sponsorship, and strive to make it apparent to consumers when they move within a site or leave one site for another.	See Hi-Ethics principles	Accredited sites must clearly indicate to users when they are leaving the site to go to a linked site. The site must disclose what types of services it provides, the terms and conditions regarding those services, appropriate uses and limitations of those services, rights and responsibilities of the users and other participants. The site must also disclose significant financial investors and interests in the owner or the site, the identity of the Web site owner, where to get more information about the owner, significant relationships with commercial sponsors, its advertising and sponsorship policies, and whether it has material financial and/or business relationships with linked sites.	Sites should clearly indicate who owns or has significant financial interest in the site, the purpose of the site or service, and any relationship a reasonable person would believe would likely influence his or her perception of the information, products, or services offered by the site. Sites should also clearly indicate when users are leaving the site.	The site is required to clearly identify support for the Web site, including commercial and noncommercial organizations that have contributed funding, services or material for the site.	Not applicable.

Table 1. Comparison of Self-regulatory Efforts by Trade Associations (continued)

	Hi-Ethics	TRUSTe and Hi-Ethics	URAC and Hi-Ethics	Internet Healthcare Coalition – eHealth Ethics Initiative	Health on the Net (HON) Foundation	eHealth Initiative (eHI)
7. Access	The site's privacy policy must provide, where appropriate, procedures for consumers to review and correct their personal information, or to request that the site delete the information and include a description of the effect of any changes on other information about the user.	See Hi-Ethics principles.	The accredited site must provide information to users about how to access, supplement and amend their personal health information.	Sites that collect personal data should make it easy for users to review their data and to update or correct it.	HONcode is silent on the issue of users' access to the personal health information they provide to Web sites.	Not applicable.
8. Security	The principles require that privacy policies contain a positive commitment from the site to use security procedures to protect personal information it collects from misuse.	See Hi-Ethics principles	The site owner must require a business partner agreement from third parties that have access to personally identifiable information on or obtained through the site. These third parties are held to the same or higher security standards as the owner of the site. If the site keeps or collects personal health information, the owner must have on file a credible auditor's report that finds the site meets or exceeds industry security standards and practices to guard against unauthorized access to the information. URAC will evaluate the credibility of the security audits case-by-case.	Sites that collect personal data should: take reasonable steps to prevent unauthorized access to or use of personal data; adopt reasonable mechanisms to trace how the data are used; and assure that when personal data are de-identified, the data cannot be linked back to the user.	HONcode does not specifically address security.	Not applicable

Table 1. Comparison of Self-regulatory Efforts by Trade Associations (continued)

	Hi-Ethics	TRUSTe and Hi-Ethics	URAC and Hi-Ethics	Internet Healthcare Coalition – eHealth Ethics Initiative	Health on the Net (HON) Foundation	eHealth Initiative (eHI)
9. Additional Restrictions or Protections	If the site collects personal health information, it will use it only for the purposes expected by a reasonable consumer. Third parties that have access to health-related personal information from the member site are required to follow the same principles. The site is also required to take appropriate precautions to prevent inadvertent disclosures of personal information to third parties and will take immediate steps to eliminate such disclosures, if they occur, once they come to the attention of the site.	See Hi-Ethics principles	The Web site cannot use personal health information for any purpose outside the scope of the opt-in. The Web site owner must require a business partner agreement from any third parties that have access to personally identifiable information on or obtained through the site. The third parties are held to the same or higher privacy standards as the site owner.	A site should make reasonable efforts to ensure that sponsors, partners, or other affiliates abide by applicable law and uphold the same ethical standards as the site itself. In addition, health care professionals who provide medical care or advice online should abide by ethical codes governing their professions in face-to-face relationships, which include: protecting patient confidentiality; disclosing sponsorships and financial incentives; and obeying relevant laws and regulations.	The site is required to respect confidentiality, honoring or exceeding legal requirements of medical/health information privacy that apply in the country and state where the site and its mirror sites are located.	Not applicable

Table 1. Comparison of Self-regulatory Efforts by Trade Associations (continued)

	Hi-Ethics	TRUSTe and Hi-Ethics	URAC and Hi-Ethics	Internet Healthcare Coalition – eHealth Ethics Initiative	Health on the Net (HON) Foundation	eHealth Initiative (eHI)
10. Remarks	The Hi-Ethics principles offer a set of rules for Web sites that offer health services, products and information to consumers. The principles address all of the criteria in this table.	The January 2000 CHCF survey found that the presence of seals of approval from Internet trade groups had no impact—positive or negative—on respondents' willingness to submit health information online.	This is the first independent accreditation program for health Web sites. It is intended for consumer-oriented, online health resources. Potential problem: accreditation fee may be prohibitive. In addition, because of the collaborative relationships among URAC, Hi-Ethics and TRUSTe, the three entities may need to make it clearer to consumers what role each of them will play. For example, will a site that participates in the eHealth seal program also be required to meet the URAC accreditation standards?	The Code was drafted and adopted after input from diverse stakeholders, both users and providers of eHealth information and services. The Code provides standards on all of the criteria in this table.	Problem: Funding is not being renewed when current contract expires in December 2001. The principles are very general and therefore offer little guidance. They do not address the specific privacy issues of notice, access, and consent. They are also silent on the issue of online security.	Unlike the other initiatives, eHI is an advocacy organization. It does not recommend codes of conduct for Web sites nor does it accredit or audit these sites.

Table 2. Comparison of Guidelines and Requirements Established by Professional Organizations

	American Medical Association (AMA)	American Health Information Management Association (AHIMA)	American Association of Health Plans (AAHP)	International Society for Mental Health Online (ISMHO)	National Board for Certified Counselors (NBCC)	National Association of Boards of Pharmacy (NABP)	International Committee of Medical Journal Editors (ICMJE)
1. Type of Initiative	Guidelines: "Guidelines for Medical and Health Information Sites on the Internet"	Principles: "Recommendations to Ensure Privacy and Quality of Personal Health Information on the Internet"	Principles: "AAHP Principles for Consumer Information in an eHealth Environment"	Principles: "Suggested Principles for the Online Provision of Mental Health Services"	Standards: "Standards for the Ethical Practice of WebCounseling"	Certification: Verified Internet Pharmacy Practice Sites (VIPPS) program	Uniform Requirements for Manuscripts Submitted to Biomedical Journals
2. Status	Guidelines were published in March 2000 to guide the development and posting of Web site content on AMA sites. A committee will review and revise the guidelines as necessary.	Released August 2000.	Approved by AAHP Board of Directors on June 5, 2000.	Principles officially endorsed by ISMHO on January 9, 2000.	The standards were last updated on June 21, 2000.	Established by NABP in spring of 1999.	A group of editors of general medical journals met in 1978 to establish guidelines for the format of manuscripts submitted to their journals. The guidelines were published in 1979. They were revised in 1997 and sections were updated in May 1999 and 2000. Over 500 journals have agreed to use the guidelines.

Table 2. Comparison of Guidelines and Requirements Established by Professional Organizations (continued)

	American Medical Association (AMA)	American Health Information Management Association (AHIMA)	American Association of Health Plans (AAHP)	International Society for Mental Health Online (ISMHO)	National Board for Certified Counselors (NBCC)	National Association of Boards of Pharmacy (NABP)	International Committee of Medical Journal Editors (ICMJE)
3. Process	The AMA policy applies to AMA Web sites – medical journals, online discussion groups, chat rooms, etc. Guidelines are expected to be operational on AMA sites.	AHIMA offers these principles as a blueprint for ensuring the privacy and quality of personal health information on the Internet.	The principles are intended for AAHP member health plans' ehealth activities. They represent only best practices.	The principles are only suggestions for addressing practice issues directly related to online provision of mental health services.	These standards are intended for use by WebCounselors. WebCounselors who are not National Certified Counselors can indicate at their Web site their adherence to these standards but they cannot publish the standards in their entirety without written permission from NBCC.	To be VIPPS certified, a pharmacy must comply with the licensing and inspection requirements of their state and each state to which they dispense pharmaceuticals. The criteria for certification include patient rights to privacy and authentication and security of prescription orders. Certified sites display the VIPPS seal. A user can view information about a specific pharmacy maintained by NABP by clicking on the VIPPS seal, which is linked to the NABP VIPPS site. The fees for participation depend on the size and type of pharmacy (i.e., community based vs. chain store) and include an application fee, annual participation fee, compliance review fee, and facility fee.	Journals that agree to use the guidelines are expected to state in their instructions to authors on how to prepare manuscripts that their requirements are in accordance with the Uniform Requirements and to cite a version of the requirements published in 1997 or later in those instructions. Guidelines also apply to electronic publishing.

Table 2. Comparison of Guidelines and Requirements Established by Professional Organizations (continued)

	American Medical Association (AMA)	American Health Information Management Association (AHIMA)	American Association of Health Plans (AAHP)	International Society for Mental Health Online (ISMHO)	National Board for Certified Counselors (NBCC)	National Association of Boards of Pharmacy (NABP)	International Committee of Medical Journal Editors (ICMJE)
4. Notice	An AMA site must provide a link to the site's privacy policy on the home page or the site navigational bar. The policy should be easily accessible to the user and the site should adhere to its privacy principles. The site should not collect personal information unless voluntarily provided by the user after the user is informed of the potential use of such information. If personal information is being collected, the site's opt in process should include explicit notice that personal information will be saved and an explanation of how the information will be used and by whom.	The notice of information practices should be conspicuously provided and in language that a layperson can understand. A Web site should inform consumers about what information is collected, by whom and how it will be used. The site should inform users of the security measures that the site uses to protect their information. The site should notify users on the screen when they enter or leave the owner's site. The site should maintain a consumer-specific log of information disclosures and make it available for review by consumers.	Health plans should disclose: their policies and procedures to use and safeguard confidentiality of personal health information and the limitations of such safeguards; and whether personal health information is collected through plans' Web sites and how the information may be used.	The client should be informed of: the potential risks of receiving mental health services online, such as breach of confidentiality; the safeguards being taken by the counselor and could be taken by the client against potential risks; any exceptions to the general rule – client information should be released only with the client's permission; and about copies or recordings of communications with the client that are being maintained by the counselor.	WebCounselors should inform Web clients of encryption methods being used to help insure security of client/counselor/supervisor communications. If encryption is not used, the client must be informed of potential hazards of unsecured communications on the Internet.WebCounselors also should inform clients if, how and how long session data are being preserved. Session data may include WebCounselor/ WebClient email, test results, audio/video session recordings, session notes and counselor/supervisor communications.	The VIPPS site only generally mentions the certification criteria, which include privacy. There are no specific standards for protecting the confidentiality of online patient health information. NABP coordinates the efforts of state and federal regulatory agencies to regulate online pharmacies.	ICMJE does not specifically address the issue of notice.

Table 2. Comparison of Guidelines and Requirements Established by Professional Organizations (continued)

	American Medical Association (AMA)	American Health Information Management Association (AHIMA)	American Association of Health Plans (AAHP)	International Society for Mental Health Online (ISMHO)	National Board for Certified Counselors (NBCC)	National Association of Boards of Pharmacy (NABP)	International Committee of Medical Journal Editors (ICMJE)
5. Choice/ Consent	AMA sites will not collect or allow third parties to collect personal medical information without the express consent of the individual after explaining the potential uses of such information. Identifying patient information should not be published unless essential for scientific purposes and the patient gave express informed consent for publication; identifying data should be omitted if not essential. Users' names and email addresses should not be released to a third party without the user's express permission. Users should be able to select whether the site will retain the username and password. Users should be able to opt in or out of functions that track personal data.	The site should provide users with meaningful opportunities to make choices about what information is collected and how the information will be used – give users right to opt in or out of specific uses and disclosures. Information should not be collected without the user's knowledge.	AAHP principles do not address consent.	Confidentiality of the client should be protected. Information about the client should be released only with the client's permission.	The WebCounseling standards do not address consent, but the NBCC Code of Ethics, which applies to all certified counselors, state that the information in counseling records belongs to the client and therefore may not be released to others without the consent of the client or when the counselor has exhausted challenges to a court order. In addition, any data derived from a client relationship and used in training or research that cannot be disguised to protect the client's identity may be used only as expressly authorized by the client's informed and uncoerced consent.	The VIPPS site only generally mentions the certification criteria, which include privacy. There are no specific standards for protecting the confidentiality of online patient health information. NABP coordinates the efforts of state and federal regulatory agencies to regulate online pharmacies.	The guidelines state that identifying information should not be published in written descriptions, photographs and pedigrees unless essential for scientific purposes and the patient (or parent or guardian) provides written informed consent for publication. The published article should indicate when informed consent has been obtained.

Table 2. Comparison of Guidelines and Requirements Established by Professional Organizations (continued)

	American Medical Association (AMA)	American Health Information Management Association (AHIMA)	American Association of Health Plans (AAHP)	International Society for Mental Health Online (ISMHO)	National Board for Certified Counselors (NBCC)	National Association of Boards of Pharmacy (NABP)	International Committee of Medical Journal Editors (ICMJE)
6. Access	AMA recommend-ations do not address users' access to personal health information they provide to a site.	The site should give users the opportu-nity to see, copy and append their records. The site should specify when, where, and how to access individually identi-fiable consumer health data that is collected and maintained but not available at the particular ehealth site.	The health plan should have a process in place to respond to or direct to the appropriate recipient consumer requests for or submission of clinically related information. (Not clear if this principle refers to general clinical information or the consumer's personal information.)	ISMHO principles do not address users' access to mental health records.	The WebCounseling standards do not address client access, but under the NBCC Code of Ethics, all records must be released to the client upon request.	The VIPPS site only generally mentions the certification criteria, which include privacy. There are no specific standards for protecting the confidentiality of online patient health information. NABP coordinates the efforts of state and federal regulatory agencies to regulate online pharmacies.	ICMJE does not address user access to personal health information they provide to a site. The focus of the ICMJE guidelines is publication of materials.
7. Transpar-ency	All financial or material support for electronic collec-tions of articles, Web site content and other types of online products should be acknow-ledged and clearly indicated on the home page or via a link from the home page. Users should be notified on-screen when they are entering or leaving a secure site and have the option to proceed or remain on the current site.	The site should clearly indicate on its home page or a page directly accessible from the home page Web site ownership or any relationships a reasonable person would believe likely to influence the site's information or services.	The health plan should disclose if it has a financial interest in a linked site and the identity of any organizations that contribute funding to the site.	Clients should be informed of the name and qualifications of a counselor. Telephone numbers or web page URLs of relevant institutions should be provided so that clients can confirm information regarding a counselor's qualifications.	The standards mention self disclosure, I.e., information about the service provider that would be available if the counseling were taking place face to face, but do not address specifically disclosures of financial interests and support.	The VIPPS site only generally mentions the certification criteria, which include privacy. There are no specific standards. NABP will coordinate the efforts of state and federal regulatory agencies to regulate online pharmacies.	At a minimum, biomedical journal sites should indicate names of editors, authors, contributors and their affiliations; reveal conflicts of interests; and disclose site ownership, sponsorship, advertising and commercial funding. In addition, it should be clearly indicated if a site links to another site because of financial considerations.

Table 2. Comparison of Guidelines and Requirements Established by Professional Organizations (continued)

	American Medical Association (AMA)	American Health Information Management Association (AHIMA)	American Association of Health Plans (AAHP)	International Society for Mental Health Online (ISMHO)	National Board for Certified Counselors (NBCC)	National Association of Boards of Pharmacy (NABP)	International Committee of Medical Journal Editors (ICMJE)
8. Security	The site should describe all security software and encryption protocol used on the site for financial transactions.	The site should obtain and maintain a list of authorized users. The site should develop, implement, and adhere to policies that define whom, how, and when data can be entered or modified. Sites should develop, implement, and adhere to a rigorous information security infrastructure – include appropriate policies, technology and architect to protect information against threats to data integrity and repudiation.	The principles state that health plans should disclose their policies and procedures to safeguard confidentiality and the limitations of those safeguards applicable to Web based systems, although it does not specifically recommend that security measures be taken and that these measures ought to meet or exceed industry standards.	ISMHO principles suggest that extra safeguards be considered when the computer is shared by others. The client should be informed of the safeguards taken by the counselor.	Standards suggest that encryption methods be used whenever possible. When it is difficult to verify the identity of the WebCounselor or client, steps should be taken to address imposter concerns. In addition, under the NBCC Code of Ethics, certified counselors must ensure that data maintained in electronic storage are secure. The data must be limited to information that is appropriate and necessary for the services being provided and accessible only to appropriate staff members. Counselors must also ensure that the electronically stored data are destroyed when it is no longer of value in providing services or required as part of clients' records.	The VIPPS site only generally mentions the certification criteria, which include privacy. There are no specific standards for protecting the confidentiality of online patient health information. NABP coordinates the efforts of state and federal regulatory agencies to regulate online pharmacies.	ICMJE guidelines do not address security issues.

Table 2. Comparison of Guidelines and Requirements Established by Professional Organizations (continued)

	American Medical Association (AMA)	American Health Information Management Association (AHIMA)	American Association of Health Plans (AAHP)	International Society for Mental Health Online (ISMHO)	National Board for Certified Counselors (NBCC)	National Association of Boards of Pharmacy (NABP)	International Committee of Medical Journal Editors (ICMJE)
9. Additional Restrictions or Protections	The site should ensure that the current technology and access possessed by third parties adhere to the site's privacy policies. The content published within an AMA site should also adhere to the patient privacy and anonymity principles followed by JAMA and the Archives Journals, which also apply to informal interactive communications on the site, including chat rooms and discussion groups.	The site should collect, maintain, and disclose data in a way that safeguards personal information and complies with federal and state laws and regulations. The site should only collect and use health information for a necessary, lawful purpose. Health information collected should be restricted to what is necessary to carry out the legitimate collections purposes. Privacy protections should follow consumers' data (chain of trust). The site should use appropriate education and training. Sites that collect or display identifiable health information should make sure that the data are documented, authenticated, corrected, stored, retained, and destroyed in a manner consistent with federal and state laws and regulations.	Health plans should promote the use of de-identified or aggregate information. Health plans should also work with vendors and practitioners to promote understanding of the plans' confidentiality standards.	No other specific protections or restrictions are mentioned, although the principles do suggest that counselors follow the laws and other established guidelines that apply to them.	WebCounselors must work to ensure the confidentiality of their Web counseling relationship—follow appropriate procedures regarding the release of information for sharing Web client information with other electronic sources. Under the NBCC Code of Ethics, the counseling relationship and information that results from that relationship remains confidential. Certified counselors are responsible for insuring that their employees handle confidential information appropriately. Confidentiality also must be maintained during the storage and disposition of records.	VIPPS pharmacies must maintain and enforce policies and procedures to assure patient confidentiality and protect patient identity and patient-specific information from inappropriate or nonessential access, use or distribution.	No other relevant protections or restrictions.

Table 2. Comparison of Guidelines and Requirements Established by Professional Organizations (continued)

	American Medical Association (AMA)	American Health Information Management Association (AHIMA)	American Association of Health Plans (AAHP)	International Society for Mental Health Online (ISMHO)	National Board for Certified Counselors (NBCC)	National Association of Boards of Pharmacy (NABP)	International Committee of Medical Journal Editors (ICMJE)
10. Remarks	The guidelines provide detailed rules for AMA Web sites that provide medical and health information, however, they do not address users' access to personal information they provide to these sites and whether they can amend or supplement that information.	AHIMA has developed detailed principles for its membership and ehealth organizations on protecting privacy and ensuring the quality of health information on the Internet. However, compliance with the principles is voluntary.	AAHP offers only general principles for its member plans. The principles do not address user control and consent.	The guidelines only focus on online delivery of mental health services so they do not address issues that may be relevant to other types of mental health sites, such as information based or patient driven sites.	The WebCounseling standards are silent on client access to records maintained by the WebCounselor and clients' consent to the disclosure of their information to others, however, they refer counselors to the NBCC Code of Ethics, which applies to all certified counselors and include standards on access and consent.	NABP does not regulate the online pharmacies. VIPPS certification is only a voluntary program for Internet pharmacies. Online sites and practitioners are regulated by the state boards of pharmacy.	ICMJE tries to apply its offline standards for journal publication to online posting of similar materials, so its application is limited.

Sources

- American Association of Health Plans, AAHP Principles for Consumer Information in an E-Health Environment (http://www.aahp.org/AAHP/Govt_Advocacy/LegacyDocs/PDF/board-5.pdf).
- American Health Information Management Association, Recommendations to Ensure Privacy and Quality of Personal Health Information on the Internet (http://www.ahima.org/infocenter/guidelines/tenets.html).
- eHealth Initiative (http://www.ehealthinitiative.org).
- Health On the Net Foundation, HON Code of Conduct (http://www.hon.ch/HONcode/Conduct.html).
- Hi-Ethics, Ethical Principles For Offering Internet Health Services to Consumers (http://www.hiethics.org/Principles/index.asp).
- International Committee of Medical Journal Editors, Uniform Requirements for Manuscripts Submitted to Biomedical Journals (http://www.icmje.org/index.html).
- International Society for Mental Health Online, Suggested Principles for the Online Provision of Mental Health Services (http://www.ismho.org/suggestions.html).
- Internet Healthcare Coalition, eHealth Ethics Initiative, eHealth Code of Ethics (http://www.ihealthcoalition.org/ethics/ehcode.html).
- National Association of Boards of Pharmacy, Verified Internet Pharmacy Practice Sites program (http://www.nabp.net/vipps/intro.asp).
- National Board for Certified Counselors, The Practice of Internet Counseling (http://www.nbcc.org/ethics/webethics.htm).
- TRUSTe and Hi-Ethics, E-Health Seal Program (http://www.truste.org/programs/pub_ehealth.html).
- URAC and Hi-Ethics, Health Web Site Accreditation (http://www.urac.org/programs/technologyhws.htm).
- M.A. Winker et al., Guidelines for Medical and Health Information Sites on the Internet American Medical Association, 283 *JAMA* 1600 (2000).