Medscape®

PRESENTATION ABSTRACT

DATE: SEPTEMBER 26, 2000

TOPIC: SELF-REGULATION OF HEALTH CARE WEB SITES

SPEAKER: MARK E. BOULDING, GENERAL COUNSEL AND EXECUTIVE VICE PRESIDENT, GOVERNMENT AND REGULATORY AFFAIRS, MEDICALOGIC/MEDSCAPE, INC.

PROGRAM: "HIPAA CONFIDENTIALITY," GIVEN AT THE HCCA'S 2000 COMPLIANCE INSTITUTE, SHERATON NEW ORLEANS

OVERVIEW

My presentation will cover the interaction of the Hi-Ethics self-regulatory code for health web sites with HIPAA, as well as some general web site privacy issues. I will also discuss special problems and sensitivities that web sites in the health care area face. I post updates to this document and slides from presentations on my own web site, www.boulding.com.

HI-ETHICS CODE

The explosive growth of the Internet and the World-Wide Web has given health care professionals and consumers access to almost limitless amounts of medical and scientific information. Some of this information is provided by the government, some is provided by individuals or charitable/academic organizations, and some is provided by commercial entities. In addition, many observers predict that some or all of traditional medical care will move online in the next few years (the online pharmacies are leading the way). In response to concerns about ethical issues and privacy of sensitive information, various self-regulatory initiatives have emerged (listed in order of first appearance of a draft):

1. The Health on the Net Foundation Code ("HonCODE"), a short and straightforward code that is largely self-policing (www.hon.ch).

2. The eHealth Ethics Code, sponsored by the Internet Healthcare Coalition (www.ihealthcoalition.org).

3. The Hi-Ethics Ethical Principles, a product of a coalition of largely commercial health web sites (www.hiethics.org)

4. The AMA Guidelines for Medical and Health Information Sites on the Internet, which come from the American Medical Association (www.ama-assn.org)

Other presentations address the HonCODE, the eHealth Code, and the AMA code. In this document, I will briefly cover the history and content of the Hi-Ethics Code.

Hi-Ethics, or Health Internet Ethics, was formed in November 1999 to address privacy, advertising and content quality issues for Internet health consumers. Member companies donated the skills and knowledge of their executive leadership to develop the principles. Because the Hi-Ethics organizations represented a significant portion of the Internet health space, they were able to make a swift and direct positive impact on the consumer's Internet health experience. According to the Media Metrix report in March, all Hi-Ethics sites listed with Media Metrix, combined, had 11.5 million unduplicated unique users or 15.9% reach of all Internet visitors.

The Hi-Ethics principles state that Hi-Ethics companies will provide online health services that reflect high quality and ethical standards, and to that end they are dedicated to meeting the goals of:

- Providing health information that is trustworthy and up-to-date;

- Clearly identifying online advertising and disclosing sponsorships or other financial relationships that significantly affect content or services;

- Keeping personal information private and secure, and employing special precautions for any personal health information; and

- Empowering consumers to distinguish online health services that follow the principles from those that do not.

The Hi-Ethics Code contains principles in the following detailed areas:

- General privacy policy: fair information practices

- Enhanced Privacy Protection for Health-Related Personal Information

- Safeguarding Consumer Privacy in Relationships with Third Parties

- Disclosure of Ownership and Financial Sponsorship

- Identifying Advertising and Health Information Content Sponsored by Third Parties

- Promotional Offers, Rebates, and Free Items or Services

- Quality of Health Information Content

- Authorship and Accountability

- Disclosure of Source and Validation for Self-Assessment Tools

- Professionalism

- Qualifications

- Transparency of Interactions, Candor and Trustworthiness

- Disclosure of Limitations

- Mechanism for Consumer Feedback

In the press release announcing the principles, Hi-Ethics members committed to becoming compliant with them by November 1, 2000. Current Hi-Ethics member companies include adam.com, allHealth.com/iVillage, America Online, AmericasDoctor, CareInsite, Discoveryhealth.com, drkoop.com, HealthCentral.com, Healtheon/WebMD, HealthGate, HEALTHvision, Healthwise, InteliHealth, LaurusHealth.com, Mediconsult/Physicians'Online, MedicaLogic/Medscape, OnHealth, PersonalMD, PlanetRx, and WellMed

PRIVACY ISSUES FOR HEALTH WEB SITES

A significant area of concern for any developer of a web site is the privacy of information collected from users. The convention on the web (not as widely followed as some would like) is to implement a privacy policy that lets people know how their information will be user. In the health care area, there are special concerns about the sensitivity of treatment information and disease state that may require the development of a more advanced form of privacy policy.

General Privacy Policy Issues

A traditional privacy policy should address the following areas (known collectively as "fair information practices"):

1. **Notice:** users should be given enough information about how their personal information will be used to make a decision concerning whether they want to use a particular web site.

2. **Choice:** Users should have a meaningful choice about how their information is used (including the choice not to use a web site at all, and to avoid collection of any data about themselves).

3. **Access:** Users should have access to information and tools that help them understand and control how their information is used.

4. **Security:** User information should be subject to appropriate protections.

5. **Contact information:** Web sites should provide an effective means of contact for users to report privacy concerns or ask questions about use of their information.

Occasionally, "Enforcement" is mentioned as an additional component, although most web site privacy policies only address enforcement by reference to third parties (for example, TRUSTe). Once a privacy policy is in place, it binds the owner of the web site to its terms. Failure to follow the policy may result in FTC or state action.

A number of online resources that can help in the creation of privacy policies exist, including one web site (from the OECD) that will actually generate a policy in response to a series of detailed questions about proposed uses of information (http://www.oecd.org/scripts/PW/PWHome.ASP). Some good general resources on web site privacy are available on the EPIC web site (www.epic.org). In addition, a special law was recently passed to protect the privacy of children online. More information is available in the attached materials or on the FTC's web site (www.ftc.gov).

Special Privacy Issues for Health Web Sites

Public scrutiny of the way health care web treat health-related information they gather from their users is increasing. Recently, the California Healthcare Foundation (http://www.chcf.org/) released the results of two projects on health care web sites:

1. A survey that found consumers distrustful of web sites when it came to sharing their personal health information.

2. A report that raised issues as to whether many health care web sites were following their own privacy policies.

The Foundation report also focused on activities of ad serving companies and identified a serious potential leak of confidential information from health care web sites to these companies. The report received national press coverage, and some of companies involved (both health care web sites and ad serving companies) are under investigation by the Federal Trade Commission.

Recently, two groups (the Internet Healthcare Coalition and Hi-Ethics) have drafted proposed codes of ethics that address the special requirements of healthcare web site privacy policies. Some suggestions for additional points for privacy policies that have come out of these and other efforts include:

1. Applying an "informed consent" model to notice to users (so that individuals receive specific notice of the type of proposed use and limitations, as opposed to a blanket statement).

2. Allowing users to amend their information or limit use of particular aspects of it on an individual basis.

3. Creating internal systems, including policies and procedures for employees, physical security systems, and audit trails, to ensure that confidential healthcare information is protected.

Many of these points are similar to requirements that will become law for health care plans, providers, and healthcare information clearinghouses under the proposed HIPAA regulations on health information privacy. In addition, HIPAA (which likely will not apply to ALL web sites), includes features like:

1. Expiration dates for consent

2. Specific forms of notice

3. Limitations on uses by partners

4. Acknowledgment of financial gain from disclosure

5. Special rules for research uses, including creation of a "privacy board" with independent members to oversee research.

Although the effective date of the HIPAA regulations is at least two years off, and even though it will not affect every health care

web site, some web sites are considering incorporating portions of the regulation into their privacy policies (to assure "best practices").

INDEX TO ATTACHED MATERIALS

1. Biography: Mark E. Boulding

2. Hi-Ethics information and Ethical Principles (from the Hi-Ethics web site, www.hiethics.com)

3. "Developing a Privacy Policy" (from the OECD web site at www.oecd.org)

4. "The OECD Privacy Policy Statement Generator" (from the OECD web site at www.oecd.org)

AUTHOR INFORMATION

I am the General Counsel and Executive Vice President, Government and Regulatory Affairs of MedicaLogic/Medscape, Inc., a provider of software and services to health care professionals and online health care information (including a web site for consumers, CBS.Healthwatch.com). Prior to joining MedicaLogic/Medscape, I was an attorney in private practice, where I specialized in health care and technology law, with a particular focus Internet-based companies, government regulation, and healthcare e-commerce.

You can reach me in the following ways:

1. By phone: 212-760-3271 or fax: 212-760-3222

2. By email: Mark_Boulding@mail.medscape.com

3. On my web site: www.boulding.com

Mark E. Boulding

Contact Information
Tel: 212.760.3271
Fax: 212.760.3222
mark_boulding@
mail.medscape.com

Work Address
MedicaLogic/Medscape, Inc.
134 W. 29th Street
New York, NY 10001

Home Page
www.boulding.com

Mr. Boulding is the General Counsel and Executive Vice President, Government and Regulatory Affairs of MedicaLogic/Medscape, Inc., an Internet company focused on delivering knowledge at the point of care. Before joining the company, he was in private practice, where he specialized in healthcare and technology law, with a focus on Internet-based companies, government regulation, and healthcare e-commerce.

Mr. Boulding is a member of the American Bar Association/Business Law Section's Cyberspace Law Committee, where he served from 1997-2000 as the co-chair of the Internet Law Subcommittee. He is a coauthor of the ABA Business Law Section's book, *Web-Linking Agreements: Contracting Strategies and Model Provisions*. Mr. Boulding also co-founded the Internet Healthcare Coalition (IHC), a nonprofit organization dedicated to education, guidance, and policymaking in the service of high-quality health care information on the Internet. Currently, Mr. Boulding serves on the Board of Directors and is the Secretary of IHC.

Among Mr. Boulding's publications are articles and book chapters on law and regulation, product labeling, and computer law, articles for the general press on use of computers, and a law review article on government authority to regulate scientific and educational information. He has presented at meetings of the American Bar Association, the Food and Drug Law Institute, the Drug Information Association, the Pharmaceutical Research and Education Institute, the Pharmaceutical Advertising Council/HMC Council, the Medical Marketing Association, and various commercial conference providers.

An honors graduate of Yale College, Mr. Boulding received his law degree *cum laude* from the University of Michigan.

Additional information concerning Mr. Boulding, as well as copies of recent publications, can be obtained from his web site.

Hi-Ethics

HEALTH INTERNET ETHICS

- Home
- About Hi-Ethics
- Members
- Principles
- How to Join
- Press Info
- FAQ
- Contact Us

Hi-Ethics, or Health Internet Ethics, is committed to ensuring that consumers can confidently Internet's potential to improve their health and that of their families. Hi-Ethics is a coalition of widely used consumer health Internet sites and information providers whose goal is to earn trust and confidence in Internet health services. By establishing the highest ethical standards, member companies can have a swift and direct positive impact on consumers' Internet healt

Hi-Ethics companies will provide online health services that reflect high quality and ethical s to that end they are dedicated to meeting the goals of:

- Providing health information that is secure and trustworthy;
- Clearly identifying online advertising and disclosing sponsorships or other financial re significantly affect our content or services;
- Keeping personal information private and secure, and employing special precautions personal health information; and
- Empowering consumers to distinguish online health services that follow our principles that do not.

The Internet provides unprecedented potential for improving personal health. Through the I can greatly improve their knowledge about their illness and help their doctors reach a more diagnosis. Consumers can better:

- Understand their treatment options and make more informed treatment decisions;
- Communicate with doctors, family members and others facing similar health concern
- Select and conveniently purchase medical services and products to meet their needs.

The Internet is a phenomenal resource for improving personal health and healthcare. Howev unprepared consumer, there also may be risks. Risks include inaccurate or undisclosed bias information, or abuse of personal information. Internet users deserve the opportunity to enjo of the health Internet without these risks. The Hi-Ethics principles will help Web sites impler standards in a broad range of areas including:

- Privacy Policies in Conformance with Fair Information Practices
- Enhanced Privacy Protection for Health-Related Personal Information
- Safeguarding Consumer Privacy in Health Web site's Relationship with Third Parties
- Disclosure of Ownership and Financial Sponsorship
- Identifying Advertising and Health Information Content Sponsored by Third Parties
- Promotional Offers, Rebates and Free Items or Services
- Accuracy and Reliability of Health Information Content; Editorial Policy
- Authorship and Accountability
- Disclosure of Source and Validation for Assessment Services
- Professional Policies on the Internet
- Qualifications

- Transparency of Interactions, Candor and Trustworthiness
- Disclosure of Limitations · Mechanism for Consumer Feedback

Hi-Ethics provides the Internet user with the consumer protection they deserve while provid
with a clear set of rules that can be successfully and accountably implemented.

Donald W. Kemper, CEO of Healthwise, Incorporated, is the chairman of Hi-Ethics. Hoga
Hartson, LLP, with leadership by Christine Varney, supports and administers Hi-Ethics acti

Hi-Ethics™

HEALTH INTERNET ETHICS

HEALTH INTERNET ETHICS:

ETHICAL PRINCIPLES FOR OFFERING

INTERNET HEALTH SERVICES TO CONSUMERS

As Hi-Ethics members, we are committed to ensuring that individual consumers can realize the full benefits of the Internet to improve their health and that of their families. To fulfill our commitment, we are dedicated to meeting the following goals:

❖ Internet health services that reflect high quality and ethical standards;

❖ Providing health information that is trustworthy and up-to-date;

❖ Clearly identifying online advertising and disclosing sponsorships or other financial relationships that significantly affect our content or services;

❖ Keeping personal information private and secure, and employing special precautions for any personal health information; and

❖ Empowering consumers to distinguish online health services that follow our principles from those that do not.

Informed by these goals, we adopt the following ethical principles. We believe that in living by these principles, we can improve the consumer's experience with online health information and services. We have provided a glossary of terms with special meanings at the end of this document.

1. **Privacy Policies**

Our members will adopt a privacy policy that is easy for consumers to find, read, and understand. Our privacy policies will —

A.   Provide users with reasonable notice of our information practices, including disclosure of —

1. collection or use of any information about the user;

2. collection or use of aggregate data; and

3. what, if any, access to personal information collected on our health web site we provide to unrelated third parties.

May 2000

B. Provide consumers with a meaningful choice on our health web site to accept or decline our proposed collection and use of personal information provided by the consumer including, if any, consent to the transfer of information to third parties.

C. Contain a positive commitment from us to use security procedures to protect personal information we collect from misuse.

D. Provide, where appropriate, procedures for consumers to review and correct their personal information that we maintain, or to request that we delete the information, and include a description of the effect of any changes on other information about the user that we maintain.

2. **Enhanced Privacy Protection for Health-Related Personal Information**

A. If we collect health-related personal information, we will only use it for the purposes for which a reasonable consumer would expect us to use it or as agreed to by the consumer.

B. We will not disclose health-related personal information to an unrelated third party and/or for unrelated purposes without first obtaining the consent of the consumer (by means of an explicit "opt-in" procedure).

C. When we make significant changes to our privacy policies that affect the use of the health-related personal information we collect, we will give notice to our users. We will not make use of information we gathered from individuals prior to a significant change in policy without first obtaining their consent for any new uses. We may also make non-significant changes to our privacy policies that will not affect our use of a consumer's personal information. We will post such changes on our health web site.

3. **Safeguarding Consumer Privacy in Relationships with Third Parties**

A. Where third parties have access to health-related personal information from our site, our agreements with these third parties will follow these principles in giving consumers notice and choice with respect to that third party's access and use.

B. Where we have relationships with third parties, we will adopt procedures to tell consumers if third parties have access to personal information about them from our site.

C. We will 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 have come to our attention.

D.   We will not allow third parties any access to non-personal individual information collected on our site unless the third party agrees that it will not use the information to identify individuals.

4.   **Disclosure of Ownership and Financial Sponsorship**

We will disclose those who have major financial interests in us or the health web sites we operate, and those who give us significant funding or other assistance. We will —

A.   Clearly state who owns any health web site we operate.

B.   Clearly identify those who hold an ownership interest of 10% or more in our company, and those whose financial contributions to our health web site represent 10% or more of the annual revenues of our company. Financial contributions mean both cash and in-kind services or materials by persons who are not otherwise identified as sponsors.

5.   **Identifying Advertising and Health Information Content Sponsored by Third Parties**

A.   We will clearly distinguish advertising from health information content, using identifying words, design, or placement. We will design our health web sites to avoid confusion between advertising and health information content.

B.   We will clearly disclose significant relationships between commercial sponsors and our health information content by identifying a sponsor's involvement in —

1.   selecting or preparing health information content that appears on our health web site, including any sponsorship of priority listings in search engine results, product listings, or other preferences in presentation of information to consumers; and

2.   any "co-branding" of health information content or Internet health services.

C.   We will provide consumers with a policy that is easy for consumers to find, read and understand regarding our acceptance of advertising and of health information content sponsored by others. Our policy will disclose —

1.   how we identify advertising and commercially sponsored health information content on our health web site;

2.   how we may obtain revenues from third parties related to advertising and health information content sponsored by others on our health web site, including advertising revenues, commissions on consumer purchases, fees

3

based on consumer use of links to other web sites, and revenues for transfer or use of information about users, including aggregate data;

3.	whether we target advertising or sponsored health information content to consumers based on information about them or their use of our health web site; and

4.	whether we intend any links to other web sites, logos, or marks of other companies, or any co-branding to constitute recommendations to the consumer.

6.	**Promotional Offers, Rebates, and Free Items or Services**

We will comply with existing federal and state laws regarding any promotions, rebates, or free or discounted offers on our health web site.

7.	**Quality of Health Information Content**

A.	We will not make claims of therapeutic benefit without reasonable support, or deliberately provide false or misleading information.

B.	We will not accept advertising or sponsored health information content that we know either contains false or misleading claims or promotes ineffective or dangerous products.

C.	We will have an editorial policy that is easy for consumers to find, read, and understand. Our editorial policy will describe procedures we use for evaluating the quality of the health information content on our health web site, whether created by us or obtained from others.

8.	**Authorship and Accountability**

A.	We will disclose any cases where we have placed health information content on our health web site because of sponsorship or other support from a third party. In addition to identifying the sponsor, we will clearly disclose significant relationships between the commercial sponsor and our health information content by identifying the sponsor's involvement with that content.

B.	Where we reproduce health information content created by third parties, we will clearly disclose the author and/or source of the material and the date of the material or its last update.

C.	Where we present health information content as the result of clinical experience or scholarly research, we will clearly disclose the actual author(s) of the health information content.

4

D. Where we create health information content for use by consumers, we will provide consumers general information about our authors and their qualifications, our editorial policy, and, if any, our expert review process.

E. Where we create health information content, we will clearly disclose the date it was created or last updated.

F. We will have a conflict of interest policy for all authors that is easy for consumers to find, read, and understand. We will disclose all affiliations and financial relationships of authors consistent with our policy.

9. Disclosure of Source and Validation for Self-Assessment Tools

A. Where we offer self-assessment tools, we will disclose their source and appropriately describe the scientific basis for their operation.

B. We will also describe how we maintain self-assessment tools, including a description of any formal evaluation process and the date of the last review or update.

10. Professionalism

A. We believe that current codes of ethics apply when health care professionals use health web sites to provide professional care. However, these codes do not apply to every interaction between a consumer and a professional. Our health web sites shall provide conspicuous and appropriate information for consumers to understand when they are and are not in an interaction with a health professional that is covered by the ethical standards of the profession.

B. Where we allow health care professionals to engage in professional care on our health web sites, we will design Internet health services to enable health care professionals to adhere to professional ethical principles in the online environment. We will continue to evolve new standards of practice to meet the changing expectations created by consumers' use of Internet health services.

C. Internet health services directed to and for use by health care professionals are beyond the scope of these principles.

11. Qualifications

A. We will provide the credentials and qualifications of persons responsible for health care services delivered via our consumer health web site. If applicable, we will also provide information about professional licensure.

B. We will disclose whether we verify information regarding health care professionals or others who provide services or information on our health web site.

5

12.   Transparency of Interactions, Candor and Trustworthiness

A.   We will inform consumers who use our Internet health services of the risks, responsibilities, and reasonable expectations associated with their use of our services. We will make sure that this information is easy for consumers to find, read, and understand.

B.   We will strive to make it apparent to consumers when they move within a site or leave one site for another and when the move changes the risks, responsibilities, and expectations associated with their activities.

13.   Disclosure of Limitations

We will advise consumers of any limitations of our health web site as a source of health care services. In particular, we will state that online health services and health information content cannot replace a health professional-patient relationship, and that consumers should always consult with a professional for diagnosis and treatment of their specific health problems.

14.   Mechanism for Consumer Feedback

We will make it easy for consumers to provide us with feedback or complaints concerning our health web sites.

* * *

Founding members of Hi-Ethics intend to implement these principles within six months. Contracts with a third party and a health web site in effect when these principles are adopted need not be amended if the health web site has a good faith belief that the contract is in compliance with the Principles set forth herein.

HI-ETHICS GLOSSARY

For purposes of the Hi-Ethics Principles--

❖ AGGREGATE DATA means personal information or non-personal individual information collected from a group of users that has been processed so that it can no longer be used to identify a single, unique individual.

❖ CO-BRANDING refers to the joint branding of a web page or section of a consumer health web site between two or more corporate entities or individuals. Co-branding may involve the joint operation of services, health information content or products that appear on a consumer health web site.

❖ HEALTH INFORMATION CONTENT includes information to help consumers stay well, prevent and manage disease, and make decisions related to health and health care, including information for making decisions about health-related products and health services. It may be in the form of data, text, graphics, audio or video, and may involve special software or hardware and programming enhancements that support interactivity. Health information content includes both materials authored by third parties (whether scholarly works by scientists and clinicians or interpretive articles prepared for consumers) as well as materials created specifically for use on a health web site.

❖ HEALTH-RELATED PERSONAL INFORMATION refers to personal information that is associated with health issues, categories, questions, and facts obtained as a result of the individual's responses and activities on a health web site.

❖ INTERNET HEALTH SERVICES means the full range of services and activities available on a consumer health web site. Examples include the sale of health care products, delivery of health care services and health information, specialized health information searches, self-assessment tools and activities, bulletin boards, chat rooms with and without participation by health professionals, and opportunities for relationships and communication with health care professionals and health plans.

❖ NON-PERSONAL INDIVIDUAL INFORMATION does not include any information that would meet the definition of personal information (below), but may include information about a specific individual's characteristics, preferences, interests, experiences, and activities disclosed by the individual to the health web site or obtained through the individual's use of the health web site.

❖ OPERATE refers to the degree of control a corporation or individual has over the operations of a consumer health web site. A corporation or individual operates a consumer health web site if the corporation or individual is primarily responsible for the material that appears on the site including, but not limited to, advertising, health information content, services and products.

❖ OPT-IN means an affirmative ability for a consumer to accept terms and conditions.

May 2000

❖ PERSONAL INFORMATION means any individually identifiable information about an individual collected online, including a first and last name, a home or other physical address, including street name and name of a city or town, an E-mail address, a telephone number, a Social Security number, or any other identifier that may permit the physical or online contacting of a specific individual.

❖ SELF-ASSESSMENT TOOLS refers to online forms that allow an individual to supply personal information and health-related information that cause interactive software programming using medical knowledge to reach conclusions that may be relevant to optimizing health care decisions or possible health outcomes.

❖ UNRELATED THIRD PARTY refers to a corporate entity or individual who acts on its own behalf and in its own interest and to carry out a purpose other than that for which the individual accessed the consumer health web site.

DEVELOPING A PRIVACY POLICY
Test our Beta version

contents

Before you begin, please read the following: this first part of the Generator aims to provide guidance on the policy and practical issues involved in the development of an organisation's privacy policy and statement. It may also guide organisations in the refinement of an existing policy. Important considerations in the development of such a policy are highlighted. Advice on conducting an internal review with the aim of establishing current privacy practices is also provided. Links to existing resources for the development of an organisation's privacy policy are made.

The OECD **cannot guarantee** that any personal privacy statement generated by an organisation through the use of the Generator meets applicable legal or self-regulatory requirements or accurately reflects the organisation's data protection practices.

ENSURE THAT YOUR PRIVACY STATEMENT IS CONSISTENT WITH YOUR PRIVACY PRACTICES AND COMPLIES WITH APPLICABLE PRIVACY REGULATION

The posting of a privacy statement can subject an organisation to **legal liability** if the organisation fails to abide by the posted statement or if the posted statement is not in compliance with local laws. Therefore, prior to posting a privacy statement organisations are strongly urged to conduct an **extensive internal review** of their data practices which covers all departments. The organisation should also conduct a review of relevant laws where they exist.

Failure to conduct such reviews may lead the organisation to misunderstand its actual data practices and the law or self-regulatory schemes which are applicable. This could result in the development of a privacy policy and statement that are inaccurate or legally insufficient, thereby subjecting the organisation to legal liability.

Start Here
- Background
- Developing a Privacy Policy
- Creating a Privacy Policy Statement
- Start the Questionnaire
- Help

Other resources
- Access the OECD Privacy Guidelines
- Access the OECD Privacy Inventory

sponsors

Daimler Chrysler

MSN Link Exchange

Microsoft Consulting Services France

Organisations must also be alert to rising consumer expectations relating to privacy and the potential of jeopardising their relationship with consumers who choose to interact with the organisation's Web site on the basis of an inaccurate privacy statement. The proper development and deployment of a privacy policy and the underlying privacy practices are becoming value-added portions of a Web site that may become positive differentiating factors and even consumer decision criteria.

Developing a privacy statement is not a simple process. Time must be taken to make sure that it is correct. The Generator is a useful tool but may not generate a policy that accurately reflects your organisation's data practices or meets applicable legal and self-regulatory requirements.

CARRY OUT AN INTERNAL REVIEW OF YOUR PRIVACY PRACTICES

An organisation in the process of developing a privacy policy must examine its data needs, analyse its actual data practices and establish clear guidelines regarding the use of collected personal data. From these guidelines a privacy statement can be generated. For the reasons stated above, organisations must take the necessary steps to ensure that their posted privacy statement/policy is consistent with their data practices and applicable laws and self-regulatory requirements where relevant.

In conducting the internal review process that is necessary to develop a privacy statement/policy, organisations should determine:

- if and how personal data are collected from external sources;
- if and how personal data are collected from internal sources;
- who in the organisation should be included in the decision making process, including to identify if and how data are collected;
- what is the purpose for collecting personal data;
- how are personal data used;
- who controls personal data once they are collected;
- if and for what purpose personal data are shared with other organisations.
- how and where personal data are stored;
- are there existing standards, guidelines, regulations which apply to the collection, control or transfer of personal data that apply to the organisation; and
- do redress mechanisms currently exist?
- do mechanisms for providing access currently exist?

The above is a short summary please refer to the sources from which this summary was derived (The sources can be found within the Web sites of SIIA, USCIB). Other useful sources include the Workbook on applying the CSA Model Code CAN/CSA-Q830.

THE OECD PRIVACY POLICY STATEMENT GENERATOR
Test our Beta version in English

The pdf version of the Generator is available in:

- French :

contents

- German :

- Japanese : Mpt and Miti

BACKGROUND TO THE OECD PRIVACY POLICY STATEMENT GENERATOR

The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980 (**OECD Privacy Guidelines**) represent an international consensus on how best to balance effective privacy protection and the free flow of information.

In furtherance of the OECD Ottawa Ministerial Privacy Declaration, the OECD has adopted a pragmatic approach and decided, in co-operation with industry, privacy experts and consumer groups, to build an 'html' experimental tool (OECD Privacy Policy Statement Generator "Generator") based on the OECD Privacy Guidelines.

It is the aim of the project to encourage the development among public and private organisations in the online environment of privacy policies and statements, and thus contribute to the online implementation of the Openness Principle in the OECD Privacy Guidelines .

Start Here
- **Background**
- Developing a Privacy Policy
- Creating a Privacy Policy Statement
- **Start the Questionnaire**
- **Help**

Other resources
- **Access the** OECD Privacy Guidelines
- **Access the** OECD Privacy Inventory

sponsors

Daimler Chrysler

MSN Link Exchange

Microsoft Consulting Services France

It is hoped that the widespread display on Web sites of privacy policy statements based on an international instrument such as the OECD Privacy Guidelines, will foster education among Web site owners. It is also hoped that the Generator will increase awareness among visitors about the privacy practices of Web sites which they browse.

WHY DEVELOP A PRIVACY POLICY AND POST A PRIVACY STATEMENT?

The protection of personal data is of increasing concern to both consumers and governments in the light of the advent and rapid increase of electronic commerce. Internet surveys have established that one reason why many consumers are reluctant to conduct business electronically is that they are worried that the privacy of their personal data is at risk.

In order for electronic commerce to achieve its full potential, organisations engaged in online activities and electronic commerce are taking and should continue to take steps to protect privacy in the online medium in order to enhance consumer trust.

Developing a privacy policy and posting a privacy statement that informs visitors to a Web site of an organisation's privacy policy is a positive step towards gaining this consumer trust, provided that the statement is accurate. Accurate privacy statements also ensure that consumers are provided with the necessary information to make informed choices regarding their personal data.

HOW CAN THE OECD PRIVACY POLICY STATEMENT GENERATOR HELP?

The first part of the OECD Generator aims to provide guidance on the policy and practical issues involved in the development of an organisation's privacy policy and statement (it may also guide organisations in the refinement of an existing policy). Important considerations in the development of such a policy are highlighted (e.g applicable national privacy requirements, the substance and scope of policy statements, the procedure to deploy and enforce them, and the legal (or other) consequences of displaying such a statement). Advice on conducting an internal review with the aim of establishing current privacy practices is also provided. Links to existing resources for development of an organisation's privacy policy are made.

The second part of the Generator takes the form of an html experimental tool. It is intended to facilitate the on-line generation by Webmasters and administrators of privacy policy statements based on their answers to a series of questions concerning their own organisation or Web site policies for processing personal data . It produces a draft pre-formatted privacy statement which must be customised by the organisation in order to accurately reflect its privacy policy.

References to the relevant principles of the OECD Privacy Guidelines are in place to alert organisations if they supply an

answer which appears to be inconsistent with the OECD Privacy Guidelines. Additional references to Convention 108 of the Council of Europe or the Directive 95/46 CE on the protection of individuals with regard to the processing of personal data and on the free movement of such data are also made, where specific requirements are set out, for those organisations that need to ensure that their privacy policy and statement comply with these instruments.

LIMITATIONS AND CONDITIONS OF USE OF THE PRIVACY POLICY STATEMENT GENERATOR

When an organisation posts its privacy statement on a Web site, the statement will be available to, and relied on by visitors globally. The OECD Generator is therefore valuable since its use as a global educational tool is endorsed by all 29 OECD Member countries.

The OECD makes the Generator freely available to all private and public organisations. The OECD respects the confidentiality of those who choose to make use of the Generator and does not collect any information on them.

The OECD requests that organisations which mention their use of the OECD Generator, make a link to this OECD Web page. The Web page presents the whole project, and specifies that the OECD's intent is to provide guidance as to how to implement the OECD Privacy Guidelines on global networks, and not to "label" any Web site as compliant with these Guidelines.

The OECD cannot guarantee that any personal privacy statement generated by an organisation through the use of the Generator meets applicable legal or self-regulatory requirements or accurately reflects the organisation's data protection practices.

• Read Developing a Privacy Policy first.
• Creating a Privacy Policy Statement
• Start the Questionnaire

OECD Home | Contact us | Help