Privacy Policies for Web Sites

Development and Implementation

Mark E. Boulding
General Counsel and VP, Regulatory Affairs
Medscape, Inc.

Presented at the Symposium on Healthcare Internet and
E-Commerce Legal, Regulatory and Ethical Issues
Washington DC - March 27, 2000

Overview of Presentation

Privacy Policies for Healthcare Web Sites

- Legal and Regulatory Background
- Why have a privacy policy at all?
  - Fair Information Practices
  - Health care intensifiers
- Creation of the policy
- Implementation and maintenance
- Looking forward

Legal and Regulatory Background

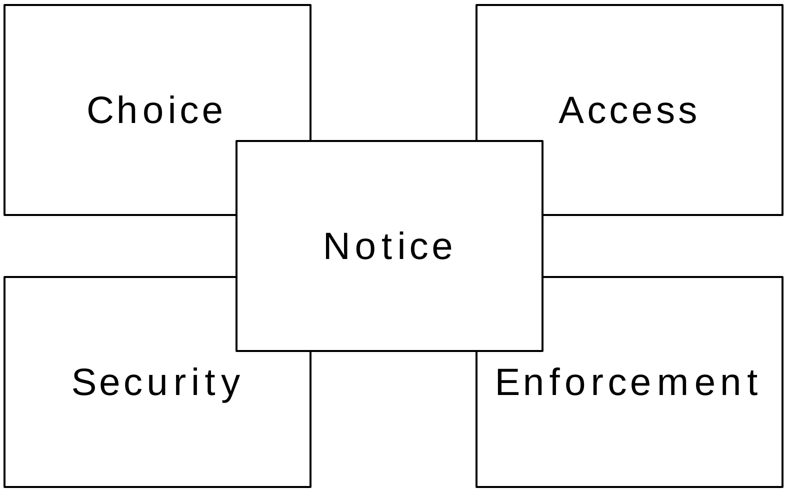
Online Privacy Protection

- State and Federal Laws
  - Patchwork approach (specific types, like video rentals)
  - Previous bills failed
- EU Directive influence in US
  - General approach to individual privacy
  - Trusted partner approach to transfers
- Specific US laws and regulations
  - Children
  - Health information (HIPAA)

History of Privacy Policies

- 1997: Most web sites did not have policies; those that did were weak (EPIC study)
- 1998: FTC report on privacy online
  - Only 14% of web sites provided notice
  - Efforts fell “far short of what is needed to protect consumers”
- 1999: Mary Culnan study of top 361 biz sites
  - 35% had no policy
  - failure to address fair information practices
- 2000: 82 of top 100 have policies (EPIC)
  - Failure to fully address fair information practices

Fair Information Practices



Notice

- Most fundamental principle
- Choice, access, enforcement depend on notice
- Required for informed consent
- Key points:
  - Who is gathering data?
  - What will it be used for?
  - Who will receive it?
  - How is it gathered? (e.g., passively)
  - Is it required or voluntary?
  - How is it protected?

Notice

A plea for plain language

- Clear and conspicuous
- Posted in prominent location
- Readily accessible from any page
- Unavoidable
- Understandable
  - "So that it gives consumers meaningful and effective notice of what will happen to the personal information they divulge" - FTC June 1998 Report to Congress

Notice - Sample Language

www.ibm.com

At IBM, we intend to give you as much control as possible over your personal information. In general, you can visit IBM on the Web without telling us who you are or revealing any information about yourself. There are times, however, when we may need information from you, such as your name and address. It is our intent to let you know before we collect personal information from you on the Internet.

If you choose to give us personal information via the Internet that we or our business partners may need ... it is our intent to let you know how we will use such information. If you tell us that you do not wish to have this information used as a basis for further contact with you, we will respect your wishes....

Notice - Sample Language

www.pathfinder.com

This site collects no personally identifying information about individuals except when specifically and knowingly provided by such individuals. An adult user's personally identifying information will not be transferred to any third party unless otherwise stated at the time of collection.

A user's personally identifying information may be used by Time Inc. for editorial purposes. Time Inc. may also use such information provided by adult users for promotional and marketing purposes.

Notice - Sample Language

www.pathfinder.com rewritten in English

We will not collect any personal information about you unless you give it to us. If we plan to give any of your personal information to anyone else, we will tell you at the time we ask for it.

We may use your personal information for editorial purposes. For example, ...

If you are an adult, we also may use your personal information to send you commercial messages.

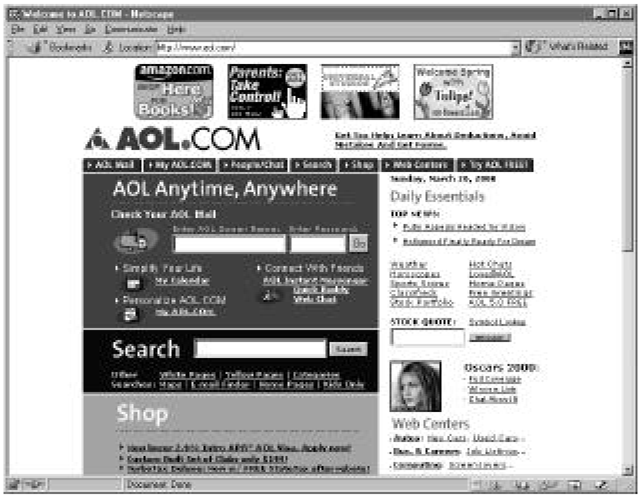
Notice - Sample Language

Hypothetical

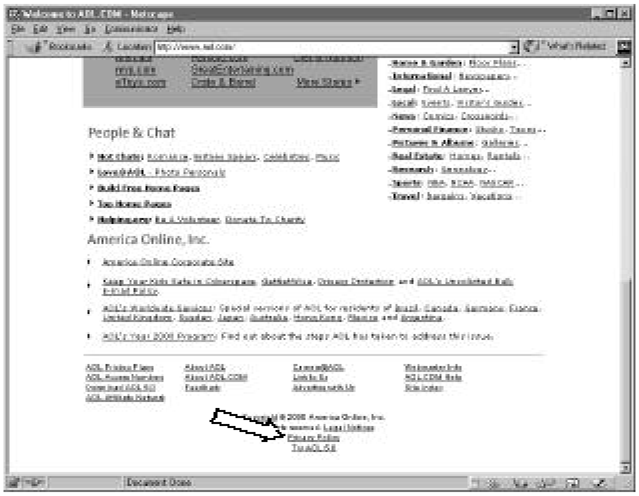
We collect information about your use of our site and any other information we can deduce from your interactions with us. We require you to provide registration data before using any portion of our site except our home page and this privacy statement.

We use information we collect about you for research and promotional purposes and to track orders you place with us. We also sell your information to third parties, and place no restrictions on their use of it.

Notice - Location of Policy



Notice - Location of Policy


Welcome to AOL.COM - Netscape
File Edit View Go Communicator Help
Bookmarks
Location: http://www.aol.com/
What's Related
Document: Done

People & Chat

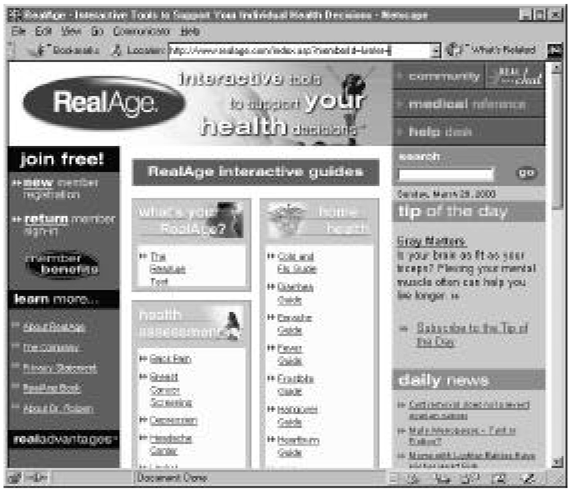
- Hot Chats: Romance, Birthday Spaces, Celebrities, Music
- Love@AOL - Photo Personals
- Build Free Home Pages
- Top Home Pages
- Helping.org: Be A Volunteer, Donate To Charity

America Online, Inc.

- America Online Corporate Site
- AOL's Worldwide Services: Special versions of AOL for residents of Brazil, Canada, Germany, France, United Kingdom, Sweden, Japan, Australia, Hong Kong, Mexico and Argentina.
- AOL's Year 2000 Program: Find out about the steps AOL has taken to address this issue.

Copyright © 2000 America Online, Inc.
All rights reserved. Legal Notices
Privacy Policy
Try AOL 5.0

Notice - Location of Policy



Sunday, March 26, 2000

Gray Matters

Is your brain as fit as your biceps? Flexing your mental muscle often can help you live longer. »

Subscribe to the Tip of the Day

Choice

- Consent to secondary uses
- "Opt-in" vs. "opt-out" (and shades between)
- Or profile based
- "Informed" consent = understanding enough to make a decision

Choice - Sample Language

www.pathfinder.com

Time Inc. may also use such information provided by adult users for promotional and marketing purposes. Individuals have the ability to stop their information from being used for marketing and promotional purposes by sending an e-mail request to Time Inc. at no_promote@timeinc.net.

Choice - Sample Language

www.drkoop.com

Our site gives users the opportunity to opt-in to receive communications from us and our partners at the point where we request information about the visitor.

This site also gives users the following options for removing their information from our database in order to stop receiving communications or our service:

[Email, snail mail, URL, and telephone]

Access

- Access by individual to information about them
- Review for accuracy and completeness
- Timely, inexpensive, and simple
- Process for verifying and forwarding corrections/objections

Access - Sample Language

Hypothetical - from TRUSTe Model Statement

If a user's personally identifiable information changes (such as your zip code), or if a user no longer desires our service, we will endeavor to provide a way to correct, update or remove that user's personal data provided to us. This can usually be done at the member information page or by emailing our Customer Support. [Some sites may also provide telephone or postal mail options for updating or correcting personal information].

Access - Sample Language

www.cbshealthwatch.com

You can choose how much information to give us, and you can edit your personal profile at any time to correct, change, or remove information. Some of our health tools may allow you share information with your other health partners, such as your physician or insurance company, but only if you decide to share the information. We also offer online interactions with other members, and you may choose to make information about yourself available to other members.

Security

- Reasonable steps
- Both managerial and technical
- Managerial:
  - Organizational procedures that limit access and
  - Prevent unauthorized use by those with access
- Technical
  - Encryption
  - Password protection
  - Firewalls and other barriers

Security - Sample Language

MedicaLogic - 98point6.com (first para only)

MedicaLogic recognizes that security for transfer of personal medical record information is of great concern to caregivers and patients alike. That is why MedicaLogic uses the Secure Sockets Layer (SSL) or other equivalent technology that ensures a secure connection from a Web browser or application to the MedicaLogic Web sites. Internet communications from one party to another may proceed via potentially unsecure computers and links, and SSL assures that data can be transmitted from one point to another without viewing or modification along the way. SSL is commonly used for financial transactions on the Internet and is generally agreed to be strong and secure protection for data being transferred. The MedicaLogic Web sites uses SSL between its customers and the Web sites whenever personal health information or financial information is transmitted. SSL is also used between systems over the Internet, such as when connecting the Electronic Medical Record (EMR) database at a healthcare enterprise and the MedicaLogic Web sites. MedicaLogic uses the domestic version of SSL (128-bit keys) to provide the strongest available protection.

Security - Sample Language

Hypothetical (from TRUSTe model statement)

While we use SSL encryption to protect sensitive information online, we also do everything in our power to protect user-information off-line. All of our users' information, not just the sensitive information mentioned above, is restricted in our offices. Only employees who need the information to perform a specific job (for example, our billing clerk or a customer service representative) are granted access to personally identifiable information. Our employees must use password-protected screen-savers when they leave their desk. When they return, they must re-enter their password to re-gain access to your information. Furthermore, ALL employees are kept up-to-date on our security and privacy practices. Every quarter, as well as any time new policies are added, our employees are notified and/or reminded about the importance we place on privacy, and what they can do to ensure our customers' information is protected. Finally, the servers that we store personally identifiable information on are kept in a secure environment, behind a locked cage.

Security - Sample Language

CBSHealthwatch.com

We have implemented technology and security policies, rules and measures to protect the personal data that we have under our control from unauthorized access, improper use, alteration, unlawful or accidental destruction, and accidental loss. We also protect your information by requiring that all our employees and others who have access to or are associated with the processing of your data to respect your confidentiality.

Enforcement

- Self-regulation
  - Trade associations
  - External audits
  - Certification schemes
- Clear path from individual complaint to resolution
- Laws and regulations

Enforcement - Sample Language

IBM.com

IBM is a member of the TRUSTe program. This statement discloses the privacy practices for the IBM Web site.

TRUSTe is an independent, non-profit initiative whose mission is to build users' trust and confidence in the Internet by promoting the principles of disclosure and informed consent. Because this site wants to demonstrate its commitment to your privacy, it has agreed to disclose its information practices and have its privacy practices reviewed and audited for compliance by TRUSTe. When you visit a Web site displaying the TRUSTe mark, you can expect to be notified of:

--What information is gathered/tracked
--How the information is used
--Who information is shared with

Questions regarding this statement should be directed to the IBM site coordinator askibm@vnet.ibm.com), or TRUSTe for clarification.

Enforcement - TRUSTe

- Criticisms based on failure to expel
- Microsoft HotMail
  - Security leak corrected
  - Audit of fix performed after public pressure
- Mothernature.com
  - Notice of failure to renew
  - Possible trademark violations
- More information:
  - www.truste.org

Enforcement - FTC Actions

FTC steps in to fill the gulf

- GeoCities
  - August 1998: FTC action charged GeoCities with misleading users about third party access to information
  - Result: consent decree - GeoCities agreed to abide by fair information practices and disclose third party access
- ReverseAuction.com
  - Harvested names from a competitor’s web site and used them to spam the users
  - Violation of eBay user agreement, deceptive statement about need to “re-register” with eBay
  - Result: consent decree with corrective measures

Self-Regulatory Systems

Alternative Enforcement for Healthcare?

- Internet Healthcare Coalition
  - Ethics summit (www.ihealthcoalition.org)
  - Code of Ethics draft
- Hi-Ethics
  - Association of “destination” health web sites
  - Limited membership
  - Draft “code” (of practice?)
- Examples of successful systems
  - US: Broadcast advertising review
  - UK: ABPI Code of Practice Authority

Health care intensifiers

- California Healthcare Foundation Reports
  - Survey of Consumer Attitudes
  - Report on Health Web Site Privacy
- Laws and regulations
  - State and federal laws
  - HIPAA and related regulatory schemes

Media Scrutiny

California Healthcare Foundation Reports

- Survey of consumer attitudes
  - Together with IHC and CyberDialogue
  - Showed increased concern about health information
  - Perception of potential for invasion of privacy
- Report on Health Web Site Privacy
  - Review of 21 major health web sites
  - Serious concerns for most
  - DoubleClick “data leaking” issue
- Extensive media coverage resulted

CHCF Survey - Personalization

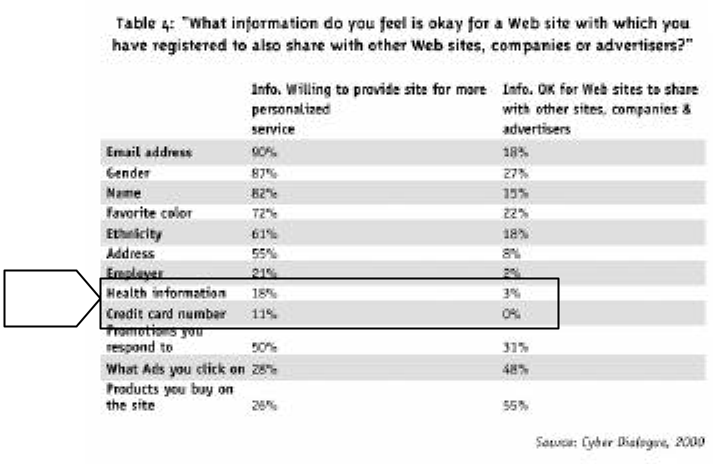
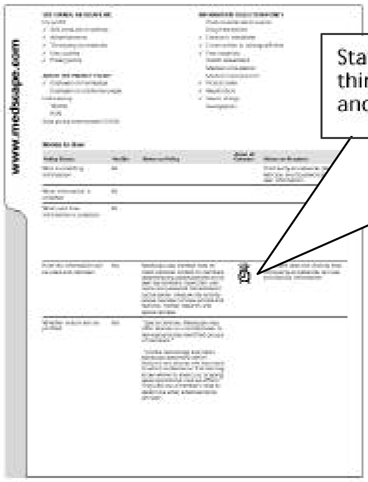


Table 4: "What information do you feel is okay for a Web site with which you have registered to also share with other Web sites, companies or advertisers?"

	Info. Willing to provide site for more personalized service	Info. OK for Web sites to share with other sites, companies & advertisers
Email address	90%	18%
Gender	87%	27%
Name	82%	15%
Favorite color	72%	22%
Ethnicity	61%	18%
Address	55%	8%
Employer	21%	2%
Health information	18%	3%
Credit card number	11%	0%
Promotions you respond to	50%	31%
What Ads you click on	28%	48%
Products you buy on the site	26%	55%

Source: Cyber Dialogue, 2000

CHCF Report - Medscape Report Card



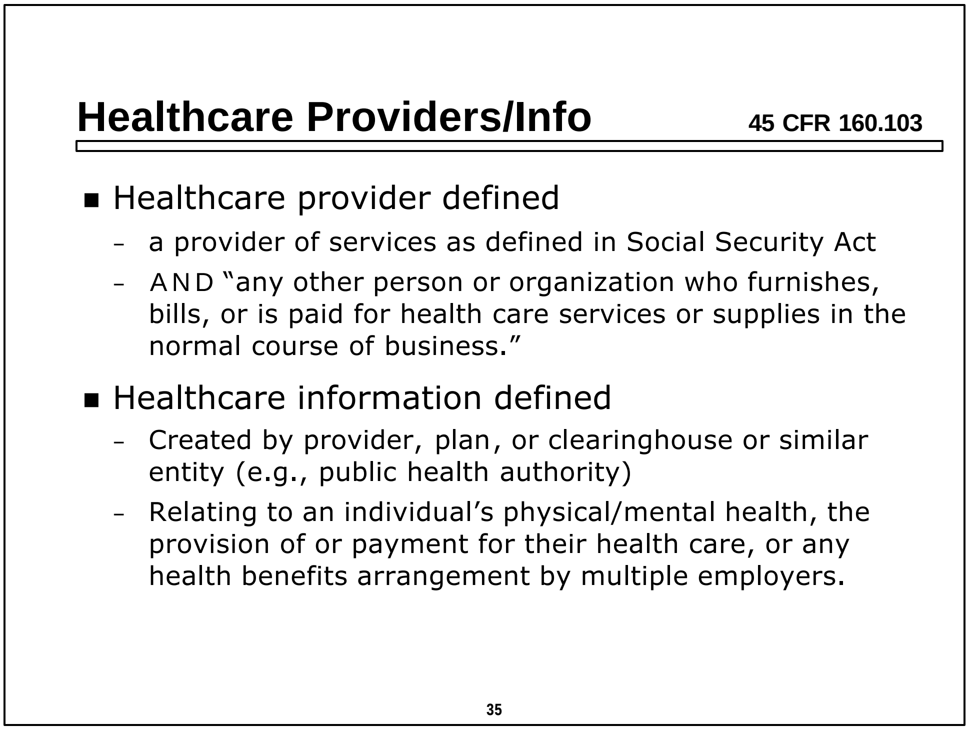
www.medscape.com

Statement does not disclose how third-party ad networks will use and disclose information.

HIPAA Coverage

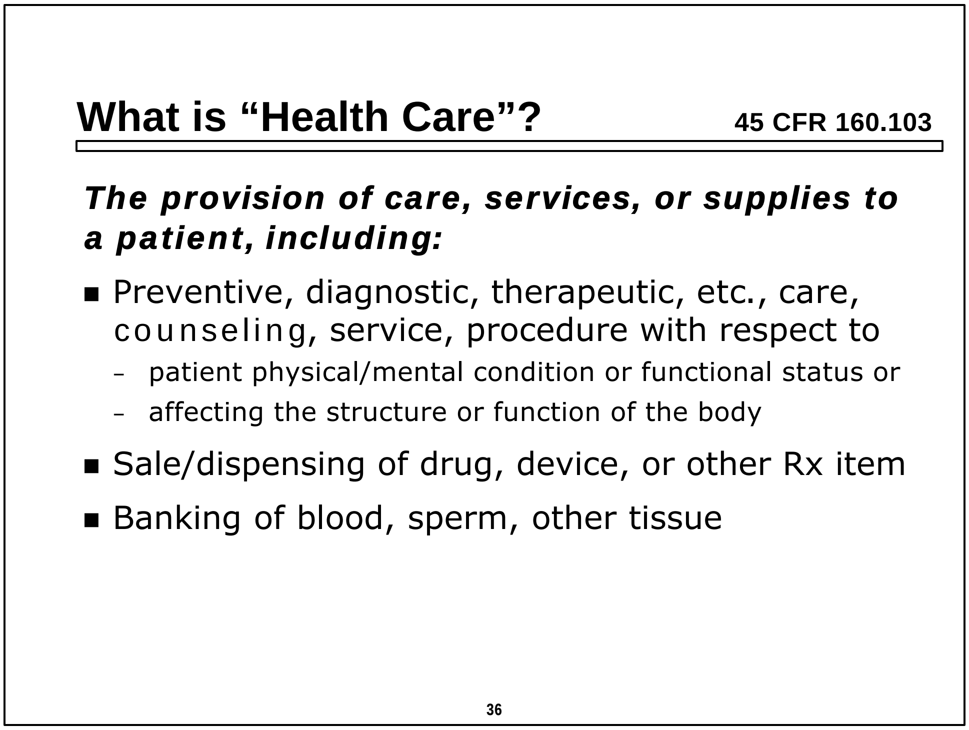
45 CFR 160.103

- Health plans
  - Special transition provisions for “small” plans
- Health care clearinghouses
  - “a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements.”
- Health care providers
  - Who transmit health info electronically
  - In connection with a covered transaction



Healthcare Providers/Info 45 CFR 160.103

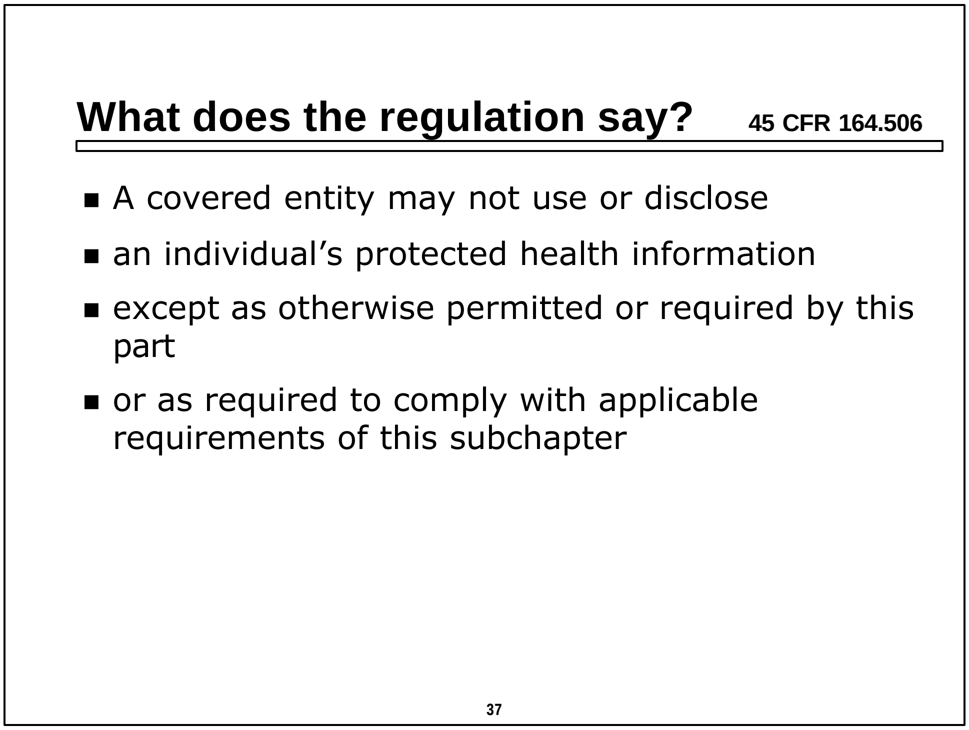
- Healthcare provider defined
  - a provider of services as defined in Social Security Act
  - AND "any other person or organization who furnishes, bills, or is paid for health care services or supplies in the normal course of business."
- Healthcare information defined
  - Created by provider, plan, or clearinghouse or similar entity (e.g., public health authority)
  - Relating to an individual's physical/mental health, the provision of or payment for their health care, or any health benefits arrangement by multiple employers.



What is "Health Care"? 45 CFR 160.103

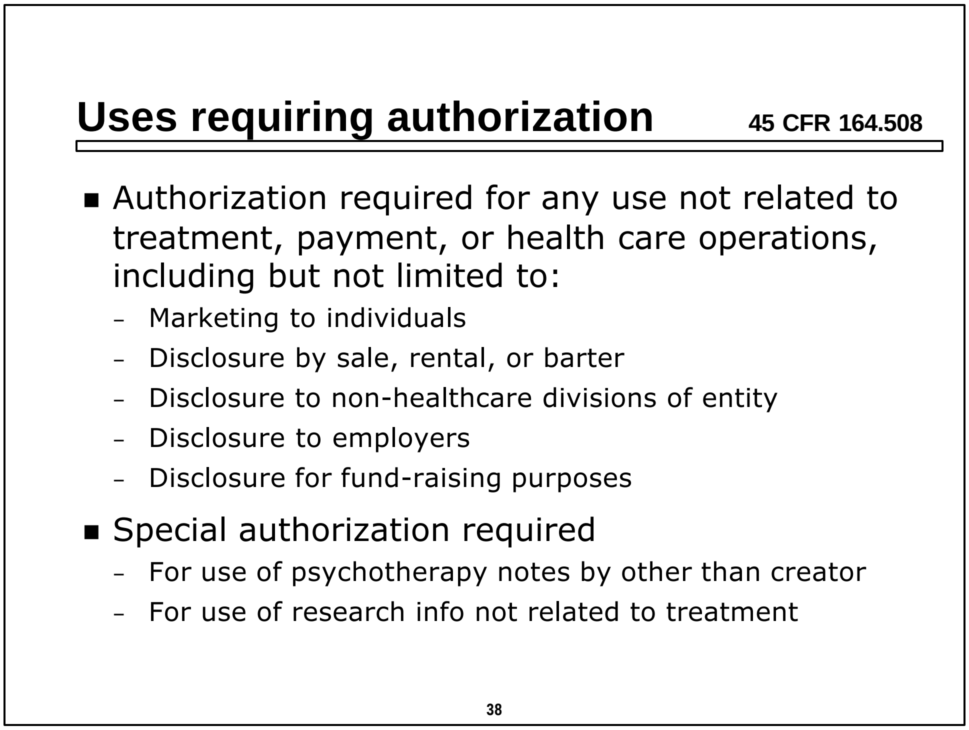
The provision of care, services, or supplies to a patient, including:

- Preventive, diagnostic, therapeutic, etc., care, counseling, service, procedure with respect to
  - patient physical/mental condition or functional status or
  - affecting the structure or function of the body
- Sale/dispensing of drug, device, or other Rx item
- Banking of blood, sperm, other tissue



What does the regulation say? 45 CFR 164.506

- A covered entity may not use or disclose
- an individual’s protected health information
- except as otherwise permitted or required by this part
- or as required to comply with applicable requirements of this subchapter



Uses requiring authorization 45 CFR 164.508

- Authorization required for any use not related to treatment, payment, or health care operations, including but not limited to:
  - Marketing to individuals
  - Disclosure by sale, rental, or barter
  - Disclosure to non-healthcare divisions of entity
  - Disclosure to employers
  - Disclosure for fund-raising purposes
- Special authorization required
  - For use of psychotherapy notes by other than creator
  - For use of research info not related to treatment

What rights do patients have?

- Notice of policies and procedures (45 CFR 164.512)
- Access to information (45 CFR 164.514)
- Accounting of disclosures (45 CFR 164.515):
- Amendment and correction (45 CFR 164.516)

Administrative requirements 45 CFR 164.518, 520

- Forms of permission, notice
- Designated privacy official, contact person
- Training of employees
- Safeguards (administrative, technical and physical)
- Documentation (6 year retention)

Health Care Intensifiers

Privacy Policy Implications

- Truly “informed” consent
  - To clinical trial level
  - Case-by-case for each use
- Better options for access and amendment
- Tighter security procedures
  - Isolation from Internet
  - Biometrics
- HIPAA?

Creation and Implementation

How do I start?

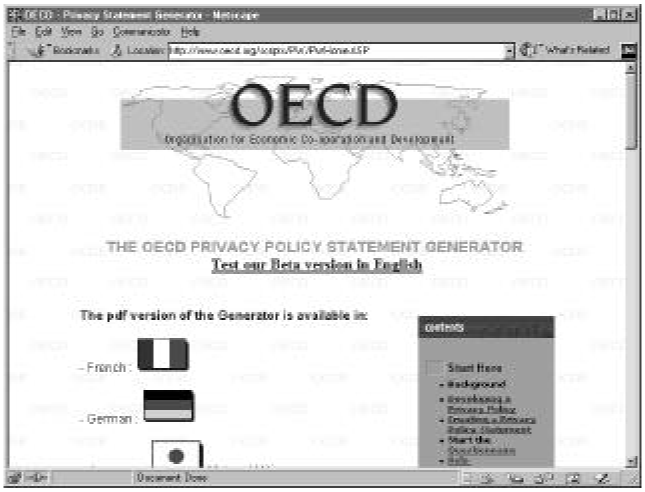
- Collect information about actual practice
- Draft policy
- Circulate to all relevant domains for review
- Appoint a privacy officer
- Develop a procedure for maintenance
- Follow legal developments (e.g., Children’s Online Protection Act)

Children’s Online Protection Act

Sample Language - 98point6.com

The 98point6 Web site is designed and intended for use by adults, and is neither intended for nor designed to be used by children under the age of 18. Minors under the age of 18 may register for 98point6 only with the prior express consent of his or her parent or legal guardian and then only under their direct supervision and responsibility. MedicaLogic and 98point6 adhere to Title XIII -- "The Children's Online Privacy Protection Act of 1998" -- and will not use any games, prizes or other activities or inducements directed at minors for any purpose, and will fully respect the privacy of the minor's personal information. We do not collect personally identifiable information from any person we actually know is a child under the age of 13. The parent or guardian of the minor is responsible for providing practical supervision to ensure the minor's authentication information is kept secure and the credibility of the health record is maintained. The parent or guardian also assumes full responsibility for the interpretation and the use of any suggestions or information provided through 98point6 by or for the minor.

OECD Privacy Statement Generator

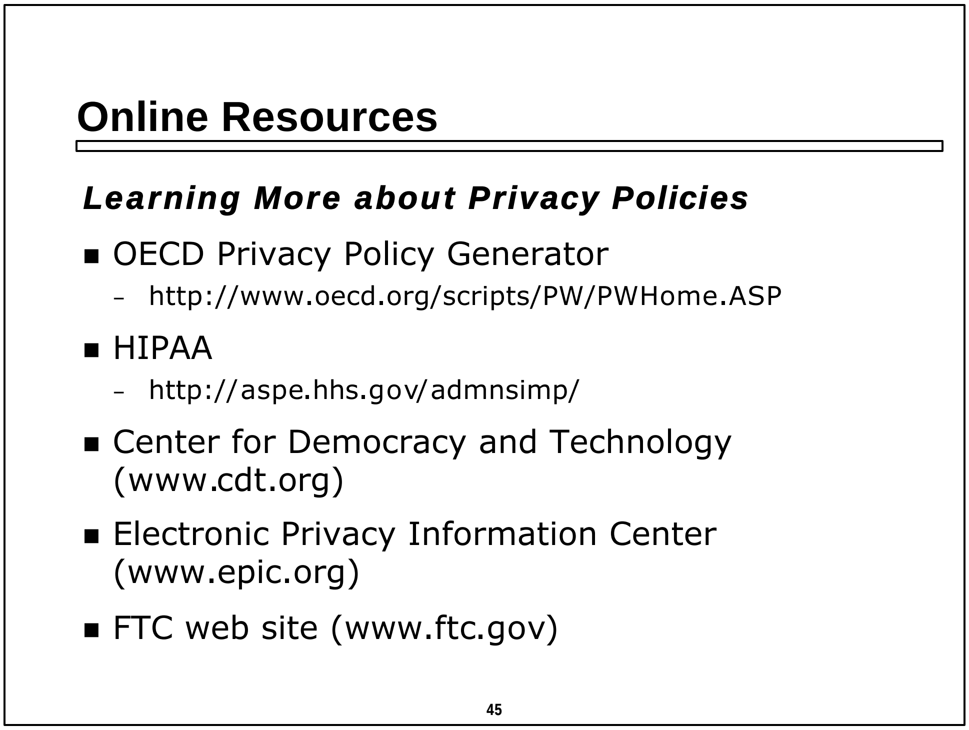

OECD - Privacy Statement Generator - Netscape
File Edit View Go Communicator Help
Bookmarks
Location: http://www.oecd.org/scripts/PW/PwHome.ASP
What's Related
OECD
Organisation for Economic Co-operation and Development
contents
Start Here
Background
Introducing a Privacy Policy
Creating a Privacy Policy Statement
Start the Questionnaire
Help
Document: Done

THE OECD PRIVACY POLICY STATEMENT GENERATOR

Test our Beta version in English

The pdf version of the Generator is available in:

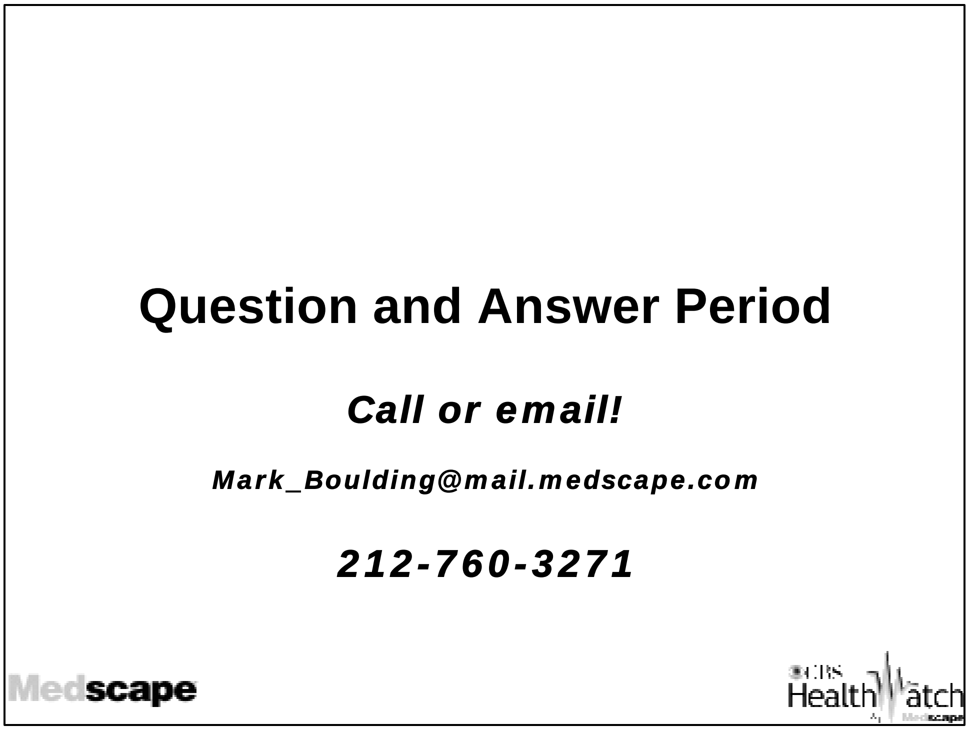
- French :
- German :



Online Resources

Learning More about Privacy Policies

- OECD Privacy Policy Generator
  - http://www.oecd.org/scripts/PW/PWHome.ASP
- HIPAA
  - http://aspe.hhs.gov/admnsimp/
- Center for Democracy and Technology (www.cdt.org)
- Electronic Privacy Information Center (www.epic.org)
- FTC web site (www.ftc.gov)



Question and Answer Period

Call or email!

Mark_Boulding@mail.medscape.com

212-760-3271