

# How to Design Online Marketing that Meets the Highest eHealth Ethics Standards

## PART 1: Gaining Pharmaceutical Consumer Trust Through Enhanced Privacy & Security

**John Mack, MS, MPhil**

President, Internet Healthcare Coalition

Publisher, *Pharma Privacy Watch*

[johnmack@virsci.com](mailto:johnmack@virsci.com)

215-504-4164



May 12, 2003 • ePharma Summit • Baltimore, MD

“e” is also for Ethics – John Mack

# How to Design Online Marketing that Meets the Highest eHealth Ethics Standards

## PART 1: Gaining Pharmaceutical Consumer Trust Through Enhanced Privacy & Security

# Pharma collects sensitive personal information from consumers

- Health web sites
- Research
- Rebate programs
- Patient assistance programs
- Targeted marketing programs
- Pharmacy compliance programs

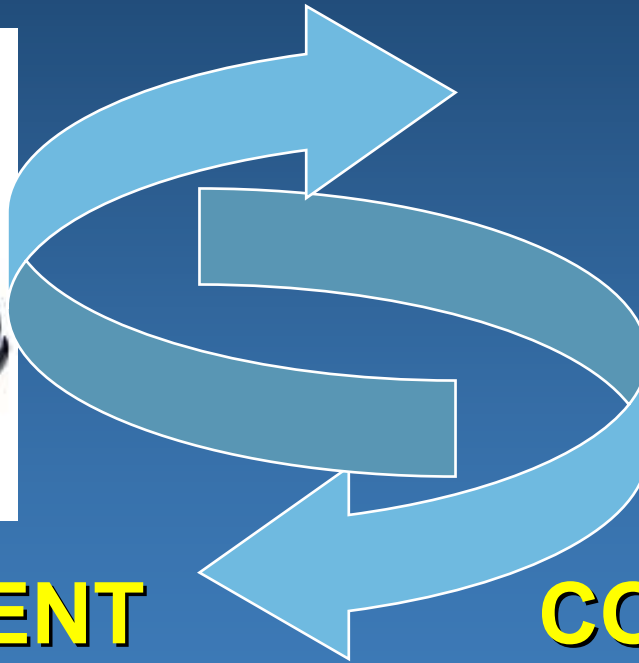
**The more data you collect, the greater the odds that you will have problems with...**



**GOVERNMENT**



**CONSUMERS**

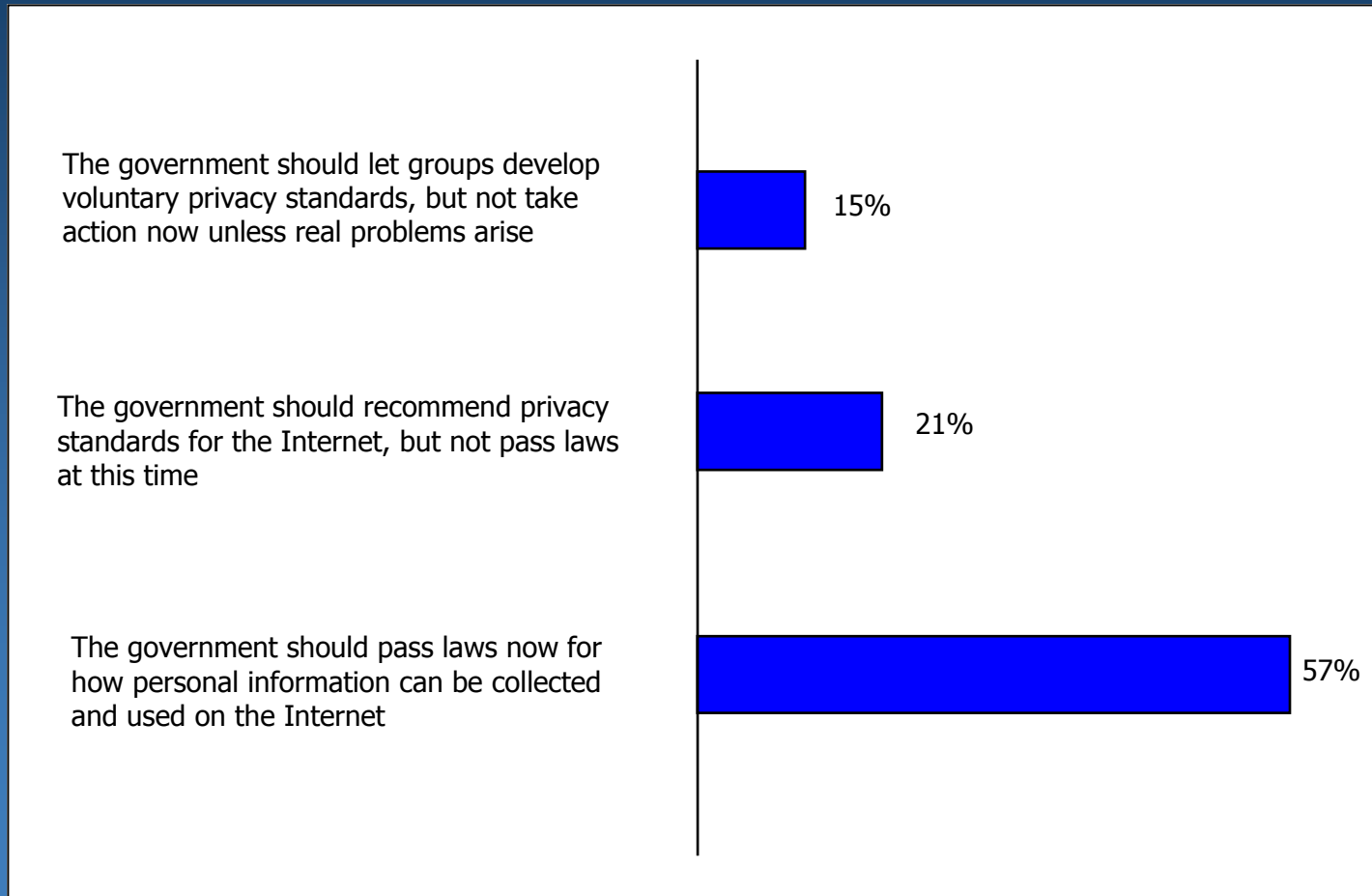


# Recent pharma privacy & security snafus validate consumer & government concerns

**“All Eli Lilly got was a slap on the  
wrist. Let's have some real  
enforcement.”**

– Sen. Hollings, sponsor of “Online Personal Privacy Act”

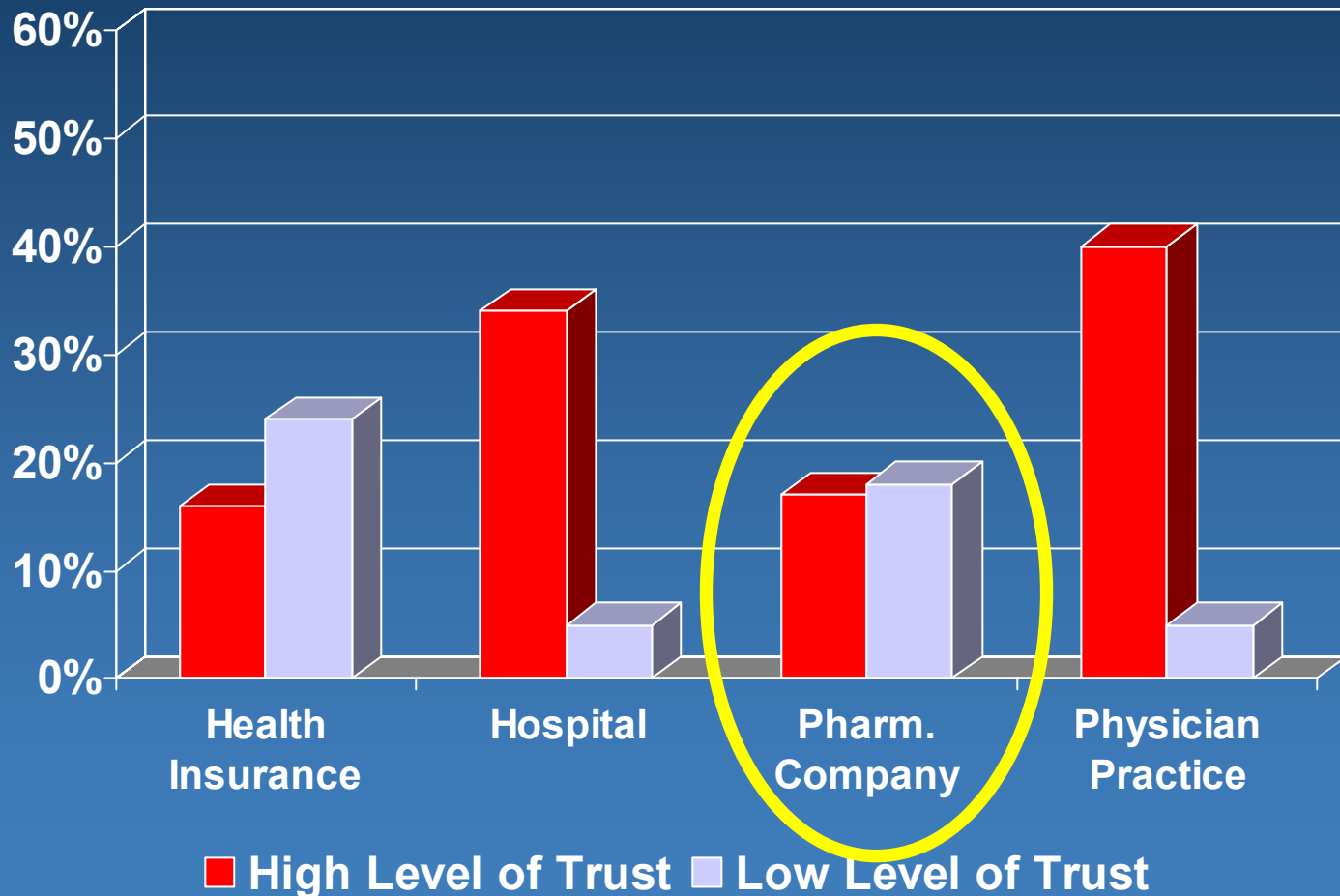
# With regard to online privacy, the public favors government intervention



Source: Harris Interactive survey of US adults, March 2000

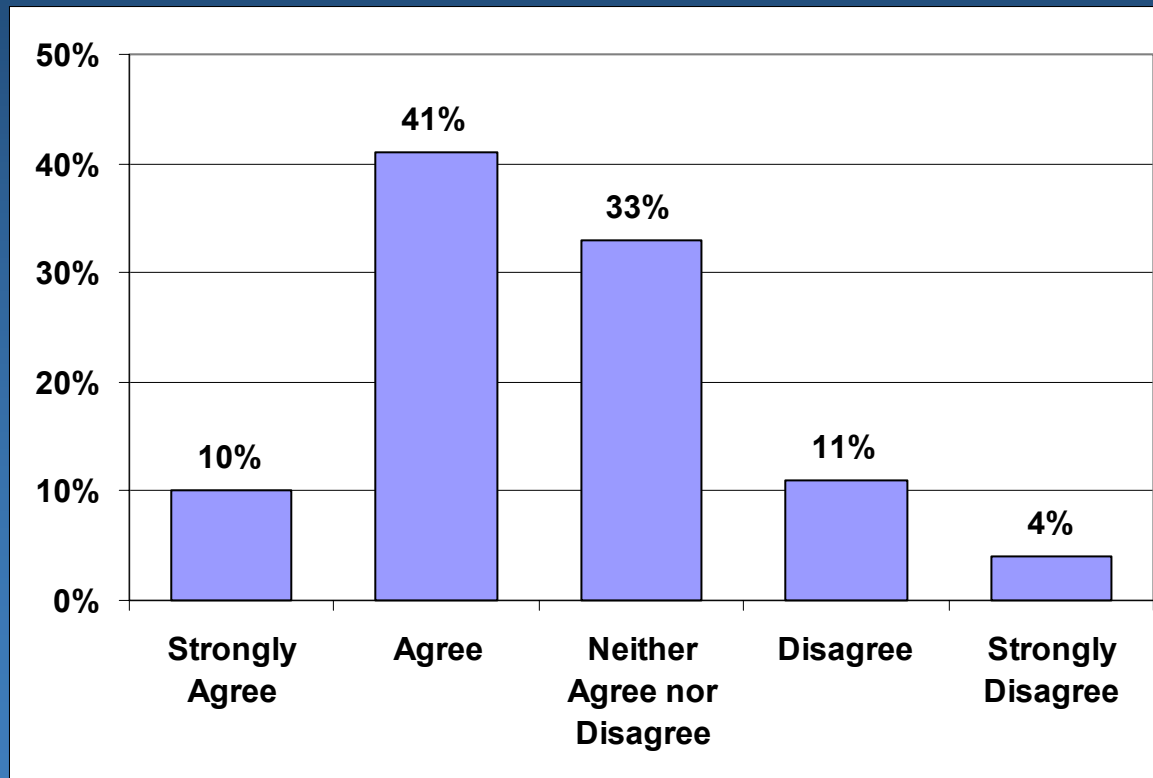
# You already have a TRUST issue....

Q: To what extent do you trust the following types of web sites?



# Although consumers are willing to share information in exchange for value...

*Percent Willing to Give Personal Information to Receive Personalized Online Experience*



Source: *Personalization Consortium*, April 2000

# Privacy is a major concern, especially among “health seekers” ...

- **Eighty-nine percent of health seekers on the Internet are concerned that a Web site might sell or give away information about what they did online.** (source: Pew Internet & American Life Project survey, 2000)
- **Only 14% of online health seekers have a “high level of trust” of Pharmaceutical company or product web sites.** (source: 2000 Cyber Dialogue survey commissioned by the Internet Healthcare Coalition and the California Healthcare Foundation)

# Why it is important to have best-in-class privacy policies and practices

- If your privacy & security practices are not in line with your public policies, FTC can take action under the “unfair or deceptive practice” rule of the Federal Trade Commission Act
- FTC will consider your online privacy policy applies to offline activities as well unless you state otherwise
- Not having a privacy policy is NOT an option – federal and state laws may require it
- **Best-in-class data collection policies and practices should HELP you build trust and increase meaningful interaction with consumers**

# **Laws & regulations that affect your business are also good places to look for data collection best practices**

- **Fair Information Practice Principles (FTC)**
- **EU Data Directive Safe Harbor**
- **HIPAA Privacy & Security Regulations**
- **COPPA**
- **State Laws**

# FTC Fair Information Practice Principles

- **Notice/Awareness**
- **Choice/Consent**
- **Access/Participation**
- **Security/Integrity**
- **Enforcement/Redress**

Source: "Privacy Online: Fair Information Practices in the Electronic Marketplace," May 2000

# EU Directive on Data Protection

- Prohibits transfer of personal data to countries that lack “adequate” privacy protection (specifically, the U.S.)
- “Safe Harbor” Concept: U.S. companies that agree to abide by seven stated privacy principles would not be prosecuted by EU member states

# Safe Harbor Privacy Principles

- **Notice**
- **Choice**
- **Onward Transfer**
- **Security**
- **Data Integrity**
- **Access**
- **Enforcement**

# Additional HIPAA Privacy Rules

- **“Minimum necessary”**
- **Consent vs. authorization**
- **Audit trail**
- **Business Associate Contract (“Chain of Trust”)**

# Notice

- *Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure. (EU Safe Harbor)*
- *Web sites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (e.g., directly or through non-obvious means such as cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site. (FTC)*

# Choice

- *Organizations must give individuals the opportunity to choose (opt out) whether their personal information is to be disclosed to a third party or to be used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For **sensitive information**, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual. (EU Safe Harbor)*
- ***Web sites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (e.g., to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities). (FTC)***

# Onward Transfer\*

- *To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the safe harbor principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles. (EU Safe Harbor)*

\* Compare to “Chain of Trust” concept under HIPAA Security NPRM

# Security

- *Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction. (EU Safe Harbor)*
- *Web sites would be required to take reasonable steps to protect the security of the information they collect from consumers. (FTC)*
- *HIPAA Security Rule consistent with “industry best practice”*
  - *Administrative and technical security*
  - *Identification and authorization*
  - *Session controls*
  - *Auditing*
  - *Physical environment*
  - *Training and awareness*

# Data Integrity

- *Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current. (EU Safe Harbor)*

# Access\*

- *Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated. (EU Safe Harbor)*
- *Web sites would be required to offer consumers reasonable access to the information a Web site has collected about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information. (FTC)*

\* Under HIPAA patients have a right to “request” amendment to data or add comments to medical record, but covered entity can refuse to make changes.

# Enforcement\*

- *In order to ensure compliance with the safe harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. (EU Safe Harbor)*
- *Among the alternative enforcement approaches are industry self-regulation; legislation that would create private remedies for consumers; and/or regulatory schemes enforceable through civil and criminal sanctions. (FTC)*

\* Under HIPAA both civil and criminal penalties can be imposed.

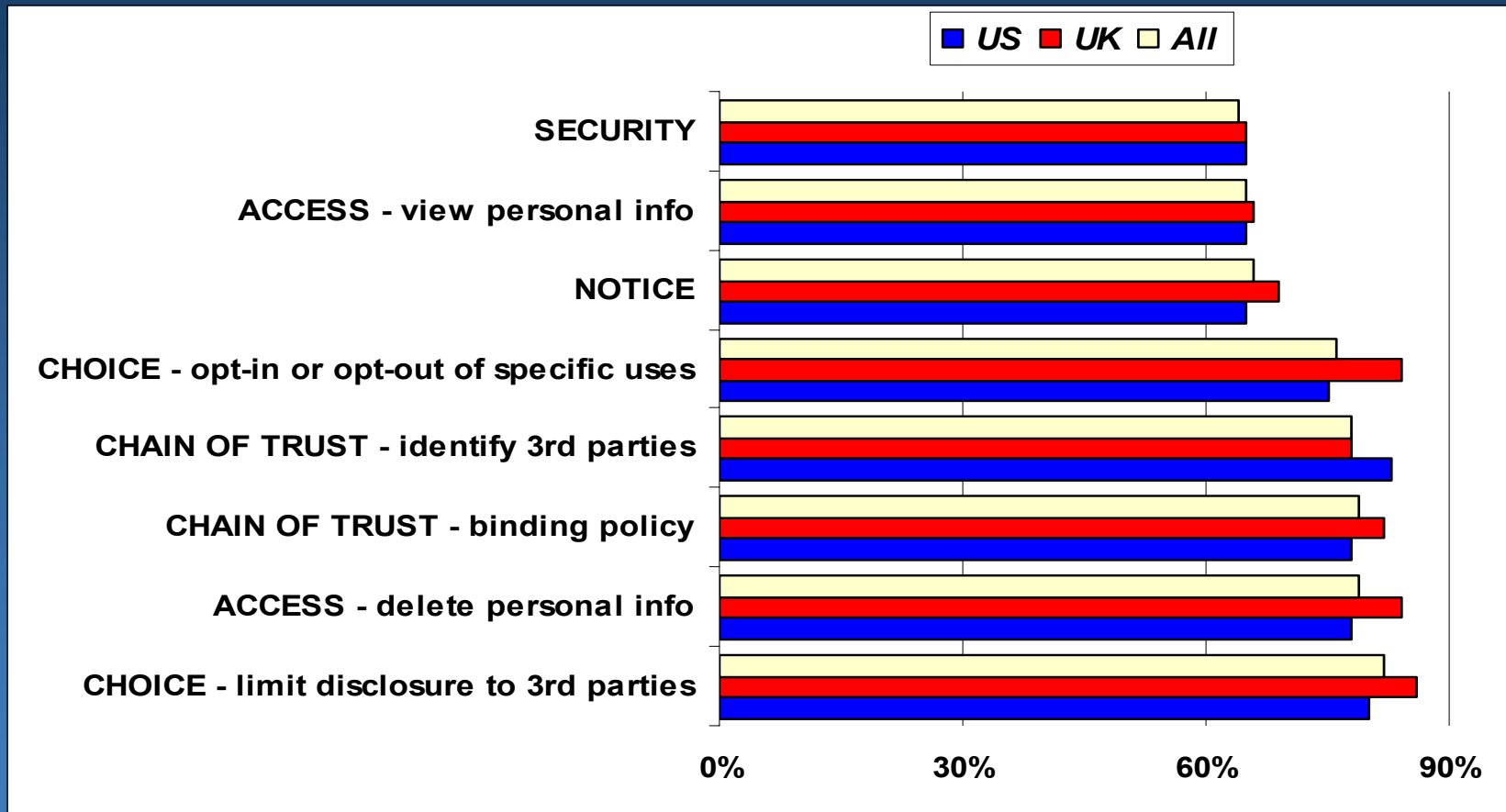
# COPPA

- If you operate a commercial Web site or an online service directed to children under 13 that collects personal information from children **or** if you operate a general audience Web site and **have actual knowledge** that you are collecting personal information from children, you must comply with the Children's Online Privacy Protection Act (COPPA).
- To determine whether a Web site is directed to children, the FTC considers several factors, including the subject matter; visual or audio content; the age of models on the site; language; whether advertising on the Web site is directed to children; **information regarding the age of the actual or intended audience**; and whether a site uses animated characters or other child-oriented features.

# Texas Medical Privacy Act

- Almost anyone who collects or maintains PHI is a “covered entity” – *including pharmaceutical companies!*
- Examples of “Covered Entity” Activities:
  - Maintaining a website
  - Research-related activities
  - Marketing activities
  - Disease management activities
- Requires compliance with HIPAA’s Privacy Standards but details of the bill, e.g., definition of marketing, differ from the final privacy rule of August 2002

# Survey of Industry Professionals: What information principles are most important for pharma-sponsored health Web sites to follow?



PollingPharma ([www.pollingpharma.com](http://www.pollingpharma.com)) January 2003 online survey of industry professionals sponsored by the Internet Healthcare Coalition and Pharma Marketing News ([www.pharma-mkting.com](http://www.pharma-mkting.com)).

Bars represent percent of respondents giving the principle the highest rating (5 or 6 on a scale of 1 to 6).

**How well does the industry  
comply with these principles?**

# Pharmaceutical Privacy Policy Compliance with Fair Information Practice Principles

## Methodology

- Access the online privacy policies of the top 20 or so Rx products
- Evaluate policy compliance with a select set of Fair Information Practice Principles (see next slide)
- Assign a numerical value of 20 for compliance with each principle and sum up to derive a “Privacy Compliance Score” (MAX=100)
- Rank products according to their Compliance Scores

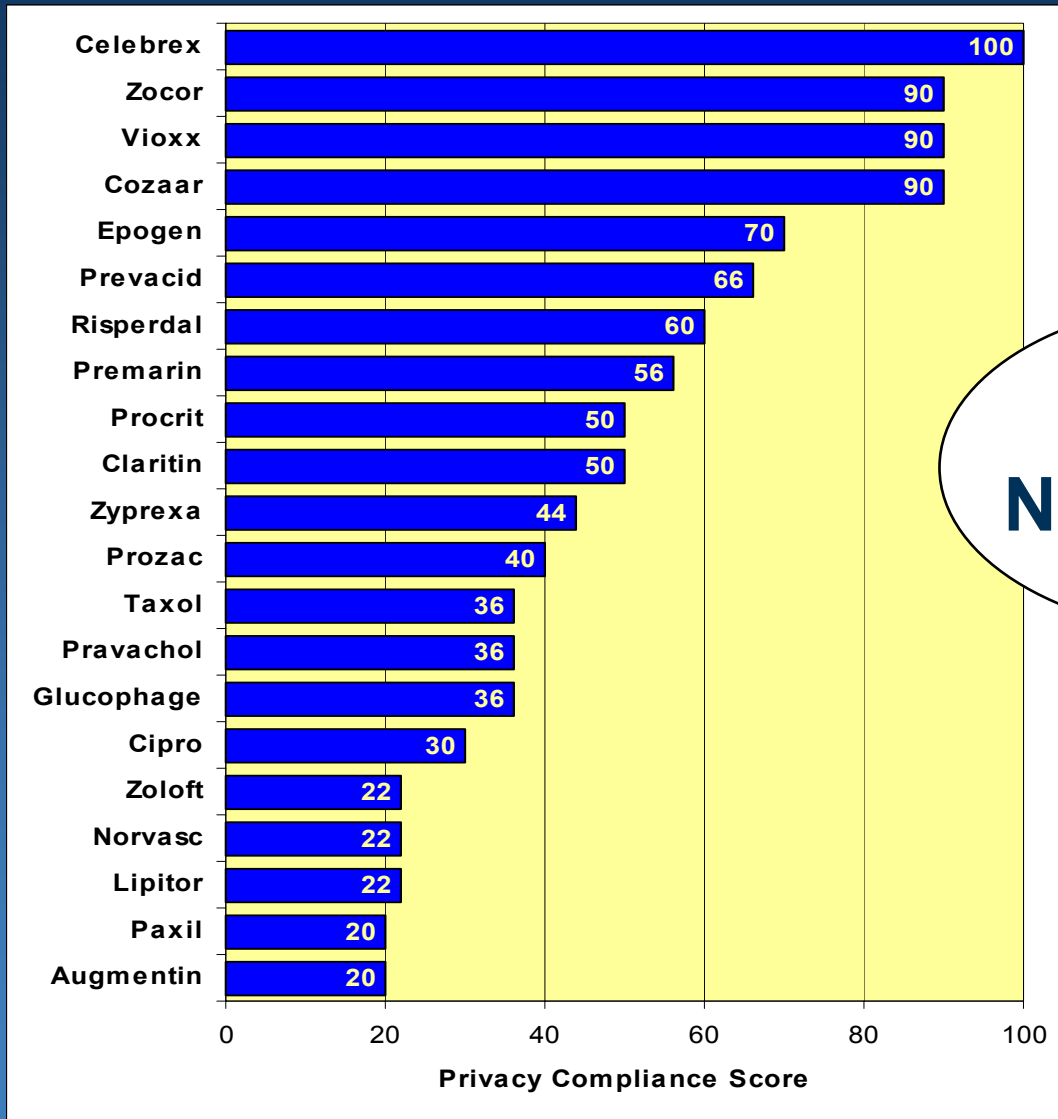
Performed February, 2002 by VirSci Corporation. As reported in *Pharma Marketing News* (2/2002) and *Medical Marketing & Media* (5/2002)

# Privacy Compliance Score

## Measurable Fair Information Practice Principles

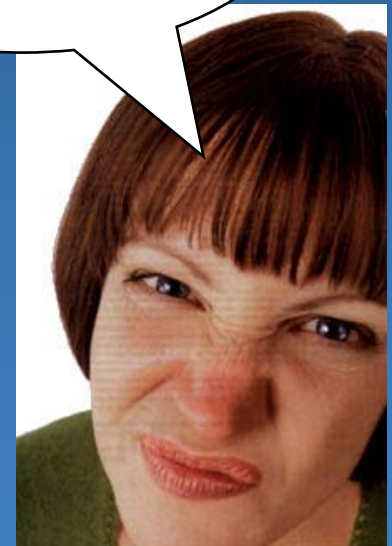
- **Notice** (20 points)
  - Who is collecting info (4)
  - What info is collected (4)
  - When and how info is collected (4)
  - How info is used or disclosed to 3rd parties (4)
  - Whether or not visitors will be profiled (“cookie” policy) (4)
- **Choice** (20 points)
  - Right to opt-in or opt-out (10)
  - Right to limit disclosure to business partners, affiliates, and other 3rd parties (10)
- **Access** (20 points)
  - Ability to view info submitted voluntarily (10)
  - Ability to correct info (10)
- **Security** (20 points)
  - Security measures explained (10)
  - Different security measures for sensitive data (10)
- **Chain of Trust** (20 points)
  - Policy binding on business partners, advertisers, etc. (20)

# Pharma Privacy Compliance Scores - 2002

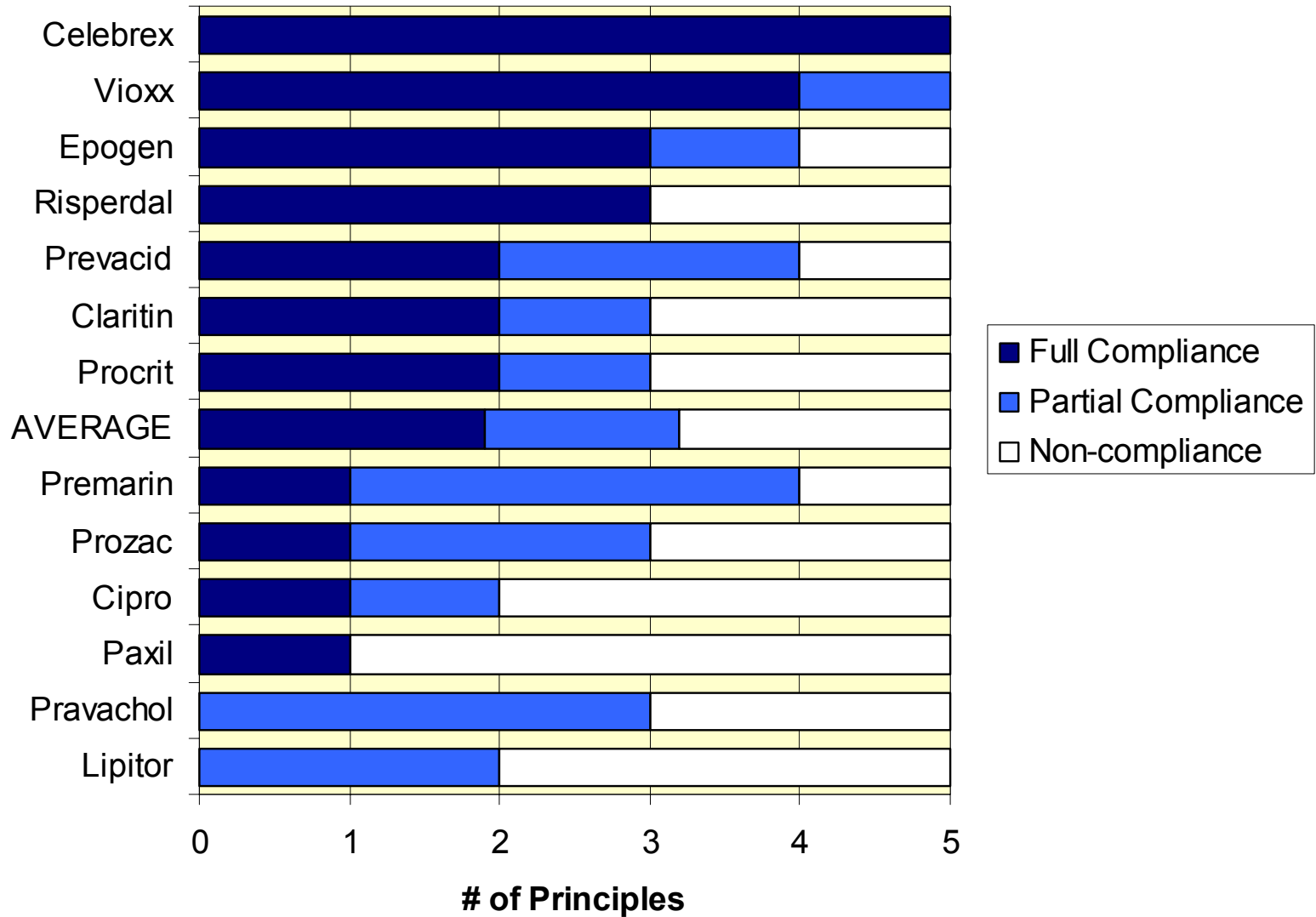


AVERAGE = 47.5

Oooh...  
Not so good!



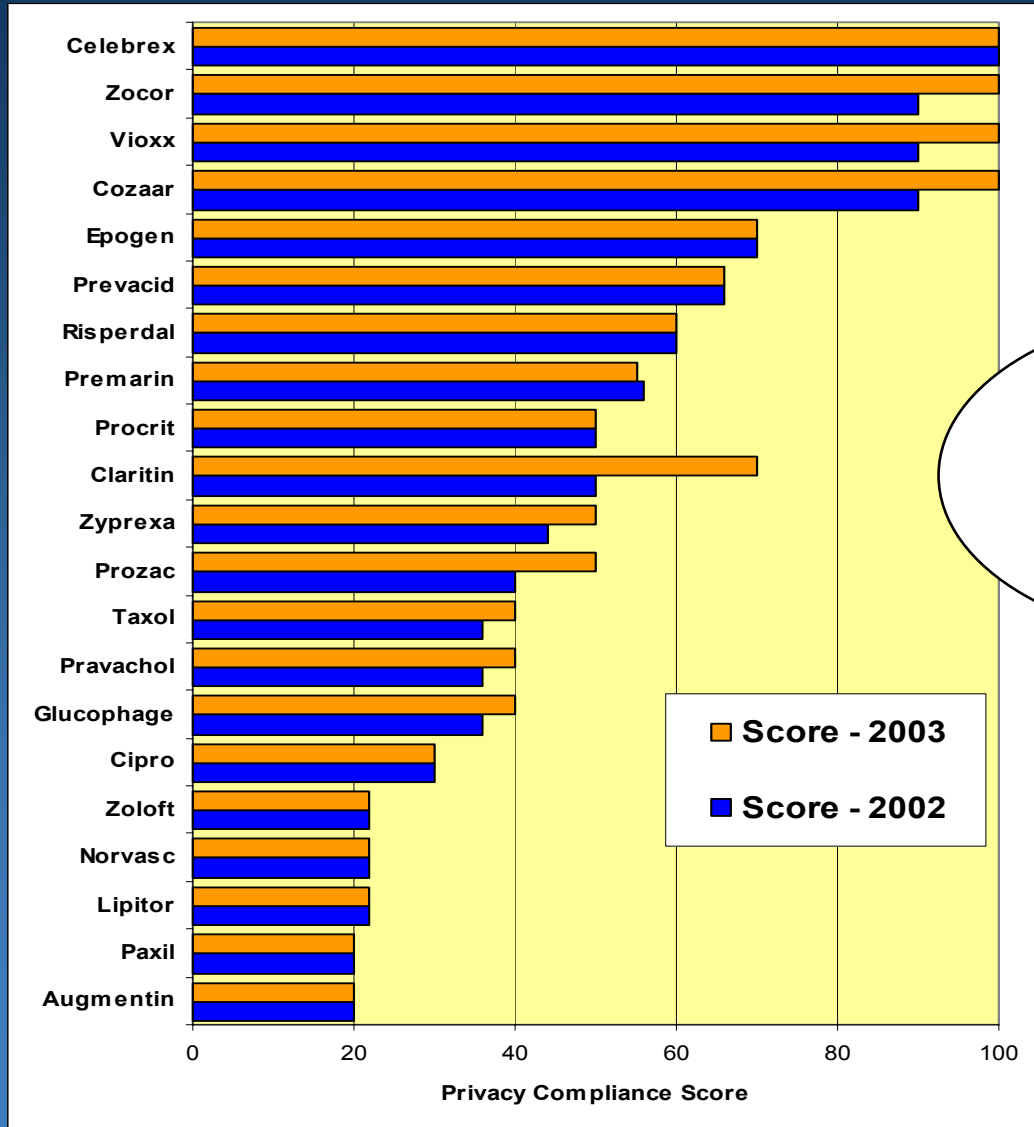
# Compliance by Product



# Fair Information Practice Compliance Summary

<i>Fair Information Practice Principle</i>	<i>Percent Full Compliance</i>	<i>Percent Partial Compliance</i>	<i>Percent Non-compliance</i>
<i>Notice</i>	69%	31%	0%
<i>Chain of Trust</i>	44%	NA	56%
<i>Access</i>	25%	31%	44%
<i>Security</i>	25%	25%	50%
<i>Choice</i>	13%	56%	31%
<i>ALL</i>	6%	94%	0%

# Pharma Privacy Compliance Scores - 2003



**Still  
not good!**



# Pharma privacy policies are not up to par

- Policies do not comply well with “Fair Information Practice” principles of FTC and EU
- Policies are often difficult to read – complex words and sentences, too long, unorganized, loaded with legal phrases
- Often does not include date last modified and unrealistic notice of revision
- Sometimes vague, especially with regard to security and chain of trust
- Link to policy difficult to find or privacy policy is buried within “Legal Disclaimer”
- Multiple, *different* conflicting policies in effect

# Suggestions for Improvement

- **Have one consistent corporate privacy policy**
  - helps to have a centralized ebusiness function or compliance/privacy officer to enforce across all brands
- **Comply with Fair Information Practice Principles**
  - move towards EU Safe Harbor and/or HIPAA as best practice
  - develop and implement *practical* written procedures for the collection of and access to information
  - implement appropriate physical, technical, and administrative security measures
  - don't forget COPPA!
- **Make sure your information collection practices comply with your policy**
- **Use trust statements *in situ* for re-inforcement**

# Trust Statements

- **Excerpts from privacy policy placed at points of data collection**
  - related specifically to specific form or application
  - can be P3P-enabled for easy content management (machine readable PP allows updates automatically when PP changes)
- **Example: self-evaluation application**
  - “The information you provide is used only to generate a customized list of questions and is not saved after you leave the site unless you choose this option and register. Your name is optional and is used to personalize the printout. If you have any questions concerning how we will or will not use your information, please consult our full Privacy Policy.”

# **A few simple general guidelines regarding personal data collection online...**

- 1. Collect personal data only if there is a clear and genuine benefit to the user.**
- 2. Collect personal data that is relevant to the benefit and commensurate to the value of the benefit.**
- 3. Collect personal data only if that data will actually be used.**

# Pharma Privacy Watch

[www.pharmaprivacywatch.com](http://www.pharmaprivacywatch.com)

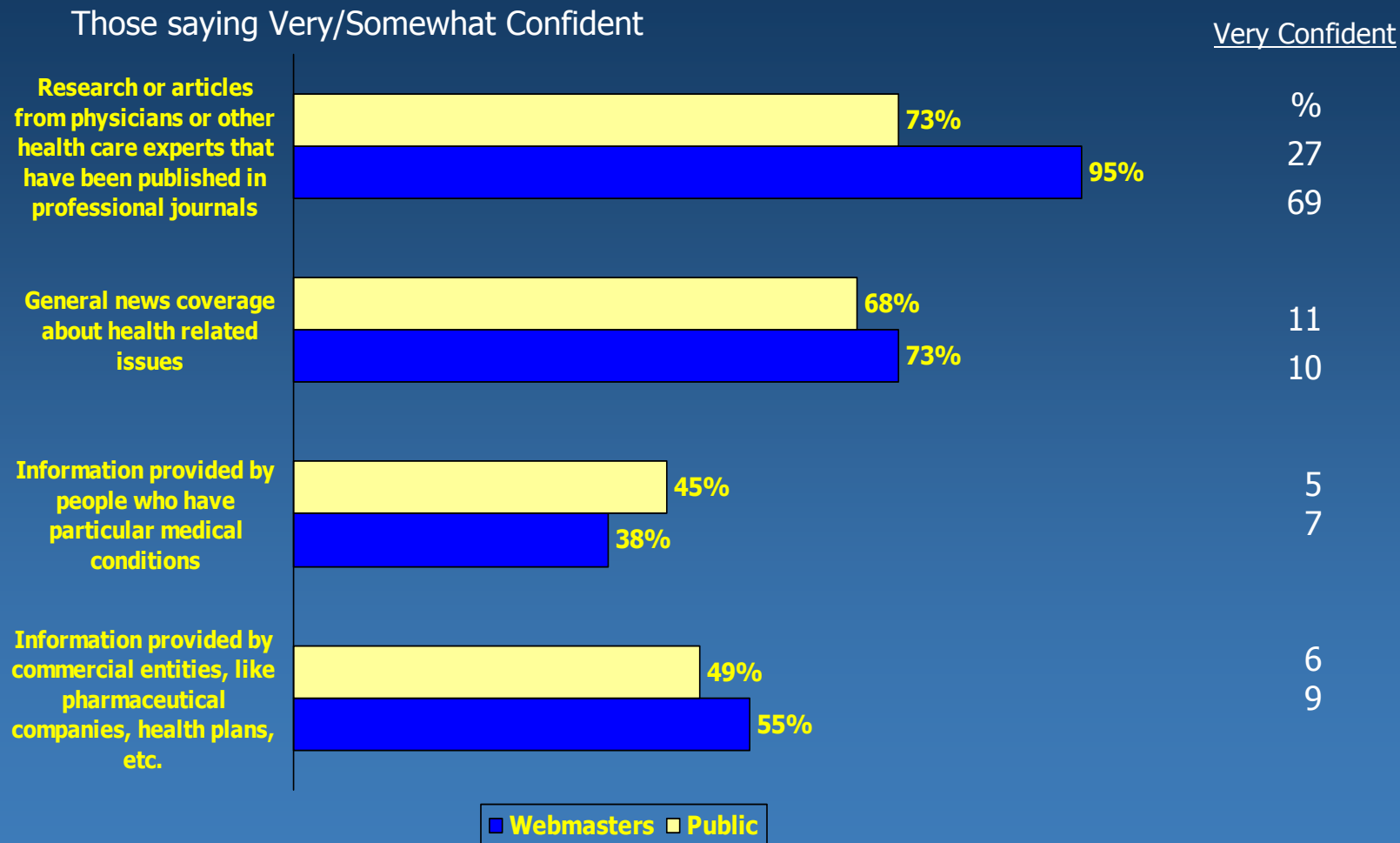


- Privacy “e-telligence” news and analysis for pharma companies
- Compares US federal, state, and EU privacy legislation with emphasis on issues relevant to the pharma industry
- News on FTC, EU and state regulatory actions
- Executive summaries, in-depth intelligence, and source documents available via e-mail and web

# How to Design Online Marketing that Meets the Highest eHealth Ethics Standards

## PART 2: Quality – Going “Beyond Regulation”

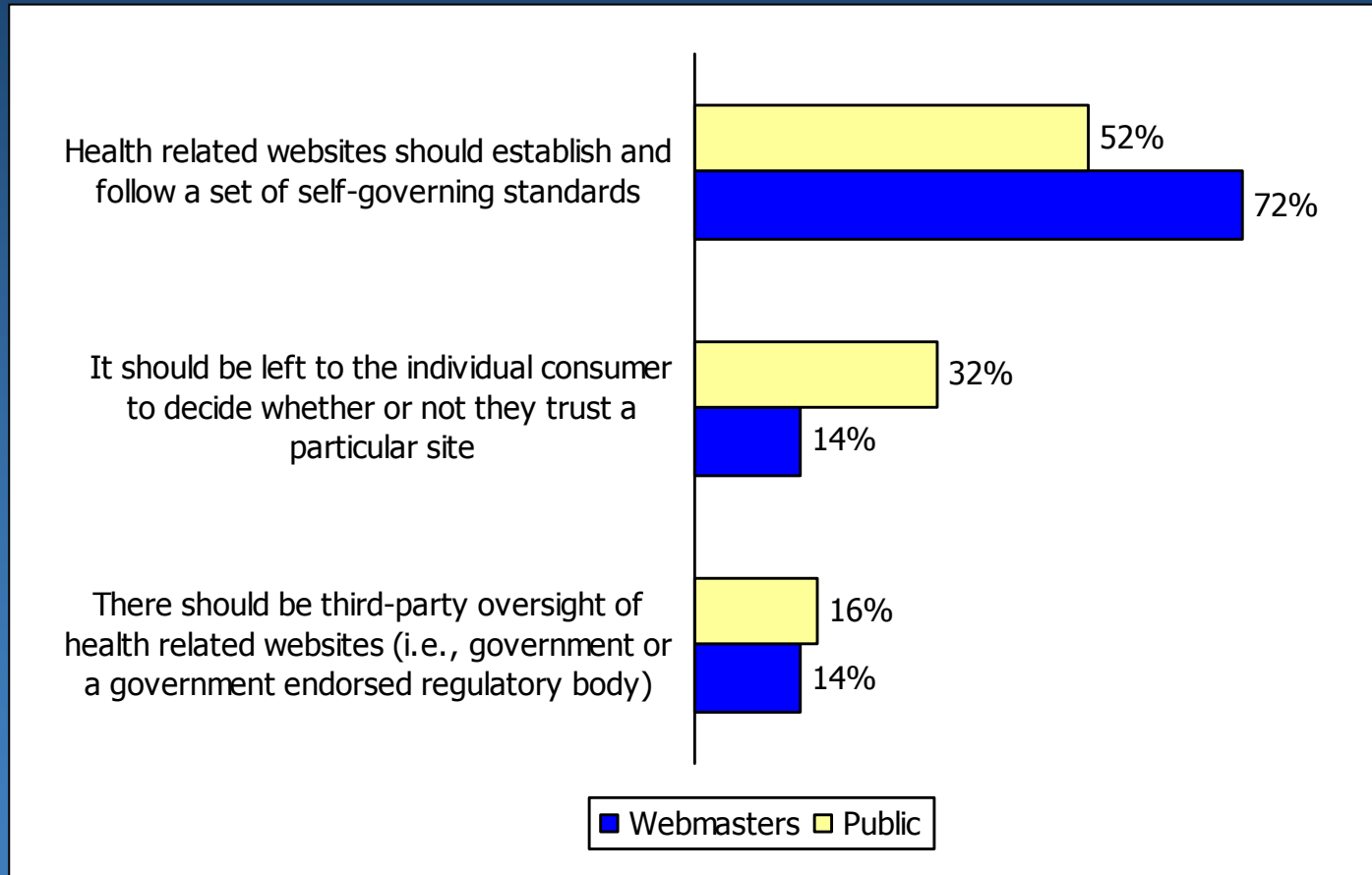
# Confidence in quality of health care information on the Internet varies by source



Q: Overall, how confident are you in the quality of the health care information that you find on these types of sites? [n=1049 (P), 101 (W)]; Internet Healthcare Coalition/Harris Interactive survey, Sept. 2000.

# With regard to quality of information, public supports self-regulation

Respondents believe Web sites should follow a set of self-governing standards.



Source: Harris Interactive/Internet Healthcare Coalition survey of US consumers vs webmasters, September 2000

# Quality of Pharma eContent

- FDA regulatory guidelines relating to fair balance
- FTC truth in advertising
- **Beyond FDA and FTC: self-regulatory initiatives**

# Quality: Beyond FDA and FTC Self-Regulatory Initiatives

- **Internet Healthcare Coalition**
  - **eHealth Code of Ethics**
- **URAC**
  - **Website accreditation program**
- **Hi-Ethics**
- **TRUSTe**
- **Health on the Net Foundation**

# Internet Healthcare Coalition



- **501c3 Non-profit formed in 1997**
- **International and broad-based membership**
- **Educational Mission**
- **Programs include:**
  - **Consumer surveys & research**
  - **eHealth Code of Ethics**
  - **Tips Program**
  - **Books and other educational activities**
  - **ehealth ethics workshops**
  - **Educational meetings, teleseminars**

# eHealth Code of Ethics

- **Consensus by open discussion**
- **Broad stakeholder participation**
- **Strong input from healthcare ethicists**
  - **Hastings Center**
  - **The Bioethics Institute (Johns Hopkins)**
- **International in scope (translated into multiple languages)**
- **Inspirational guidelines for entire Internet health arena (e.g., URAC, NMHA)**

# eHealth Code of Ethics: Principles

- **Candor**
  - Ownership, financial disclosures
- **Honesty**
  - Truthful claims, no fraud
- **Quality**
  - Accurate, easy to understand, up to date
- **Professionalism in Online Health Care**
  - Disclose credentials, describe constraints

# eHealth Code of Ethics: Principles

*Continued...*

## Privacy-Related Principles

- **Privacy**
  - Provide security, access, audit
- **Informed Consent**
  - Disclose data collected, data sharing, opt-in
- **Responsible Partnering**
  - Linking policy, choose ethical partners
- **Accountability**
  - Provide means for contact and feedback

# eHealth Code of Ethics

## Privacy & Security

- take reasonable steps to prevent unauthorized access to or use of personal data (security)
- make it easy for users to review and update personal data
- adopt reasonable mechanisms to trace how personal data is used (audit trail)
- tell how the site stores users' personal data and for how long it stores that data
- assure that when personal data is “de-identified” it cannot be linked back to the user

# eHealth Code of Ethics

## Informed Consent

- **Clearly disclose**
  - that there are potential risks to users' privacy on the Internet
  - what data is being collected when users visit the site
  - who is collecting that data
  - how the site will use that data
  - whether the site knowingly shares data with other organizations or individuals and if so, what data it shares
  - what consequences there may be when a visitor refuses to
- **Obtain users affirmative consent to collect, use, or share personal data in the ways described**

# eHealth Code of Ethics

## Responsible Partnering

- **make reasonable efforts to ensure that sponsors, partners, or other affiliates abide by applicable law and uphold the same ethical standards as you do**
- **insist that current or prospective sponsors not influence the way search results are displayed for specific information on key words or topics**
- **indicate clearly to users**
  - **whether links to other sites are provided for information only or are endorsements of those other sites**
  - **when they are leaving the site**

# eHealth Code of Ethics

## Accountability

- **indicate clearly to users how they can contact the owner of the site or service and/or the party responsible for managing the site or service**
- **provide easy-to-use tools for visitors to give feedback about the site and the quality of its information, products, or services**
- **review complaints from users promptly and respond in a timely and appropriate manner**

# About URAC

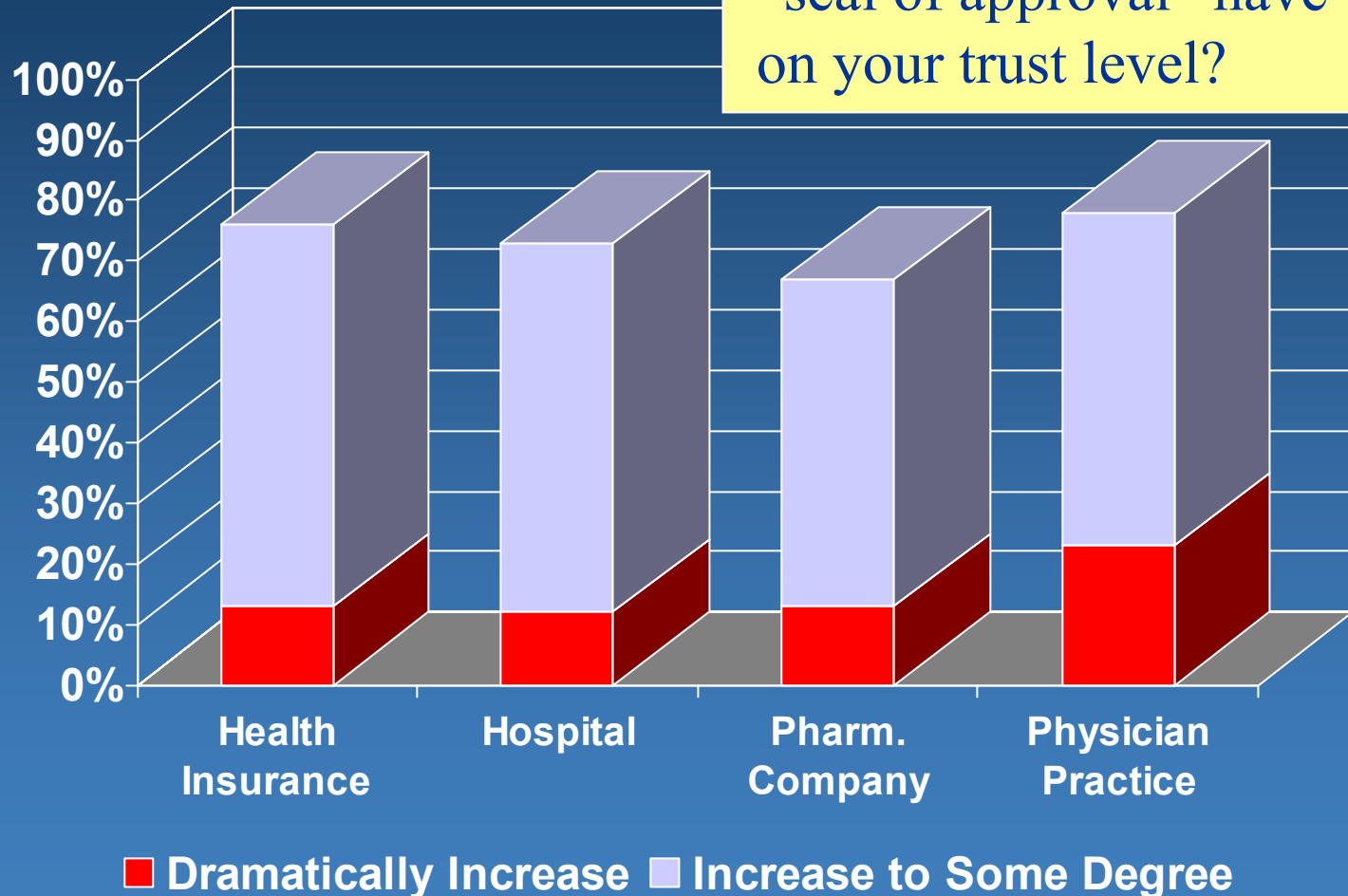
- **Non-profit, private organization**
- **Founded in 1990**
- **Accredits a broad range of health care functions**
- **In July 2001, released accreditation standards for health Web sites (program now in implementation phase)**
- **[www.urac.org](http://www.urac.org)**



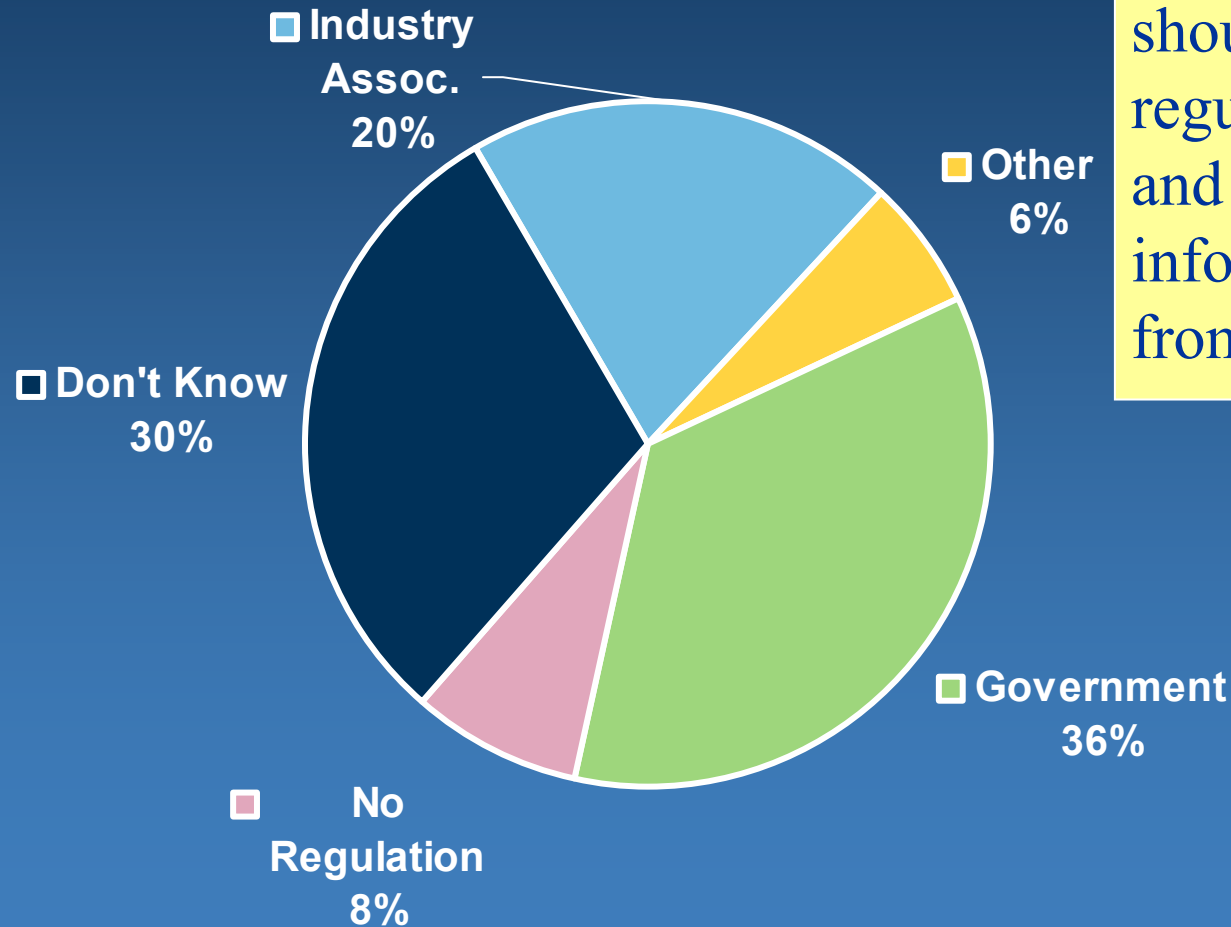
# Defining the Response

*Source: URAC*

Q: What effect would a “seal of approval” have on your trust level?



# Defining the Response

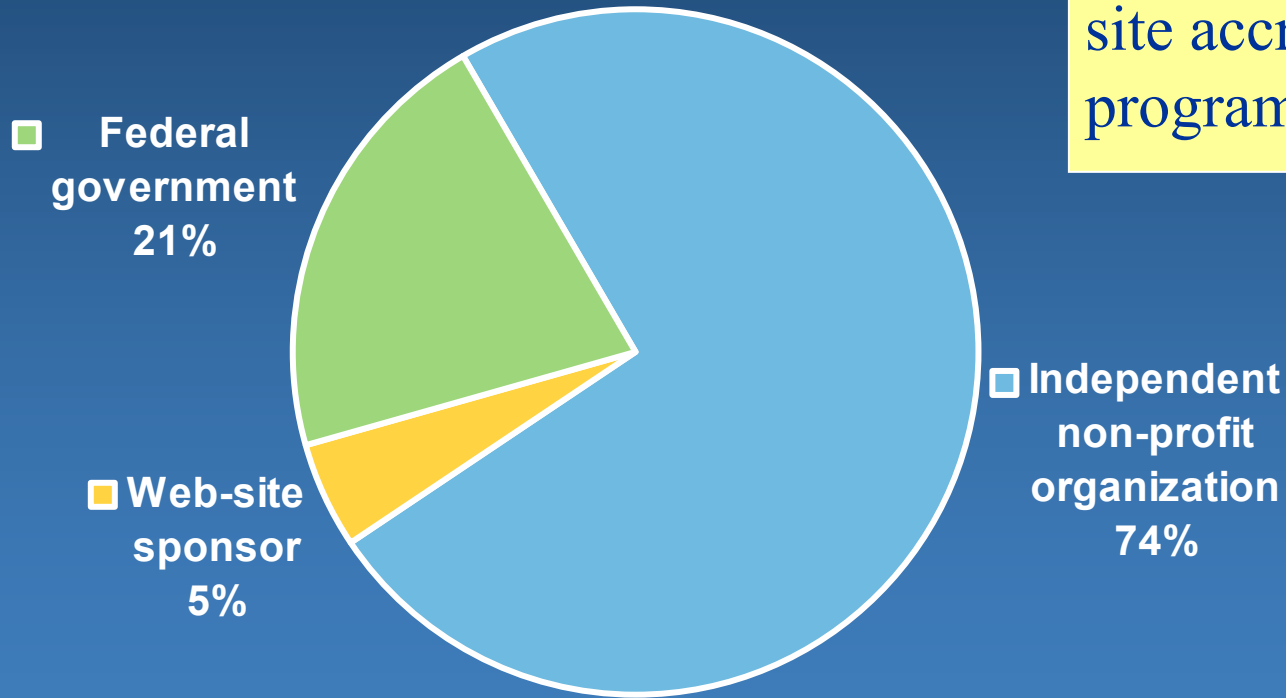


Q: Who do you think should be responsible for regulating health sites and the way they use information obtained from visitors?

*Source: CHCF*

# Defining the Response

Q: Which of the following do you most trust to administer a web site accreditation program?



*Source: URAC*

# Program Goals

- **Provide value to accredited Web sites**
  - **Mark of distinction**
  - **Marketing advantage**
  - **Quality improvement**
- **Build recognition among consumers and other stakeholders**
- **Provide platform for eHealth community to implement best practices**



# eHealth Ethics Training

- **For Executives**
  - define and shape a leadership role in fostering ethical climate and behavior
- **For Management**
  - to encourage management to model ethical behavior
- **For Employees**
  - to help employees understand and meet organizational expectations (e.g., policies)
  - help employees recognize and resolve ethical dilemmas

# Consumer Education – IHCC's Tips Program

- **Continuing Consumer Education**
  - Provide consumers a “fishing pole instead of a fish” – tools they need to find credible, balanced health information on the Net, not a list of recommended sites
- **Corporate Membership**
  - Display Coalition's logo and link to *Tips for Healthy Surfing Online*