Making health manageable.

Ethical Issues in Health Care Internet Privacy and Data Security

HIPAA Conference
October 16, 2000

Michael J. Rozen, MD
Vice President Consumer Affairs
Chief Privacy Officer
michaelr@wellmed.com

We are in the very early stages of health care informatics—just climbing out of the primordial cyber soup to blink like kids at the future and all its potential.”

Howard Bell

Writer, Healthcare Informatics

Feb, 2000

Connectivity, Communication, Convenience

Chronically Ill

Recently Diagnosed

Friends & Family

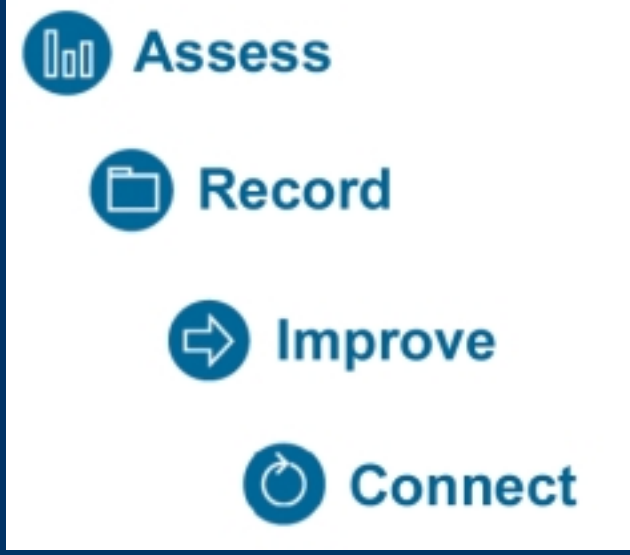
Worried Well

Health Savant

US Adults on Web
114 Million
86% looking for health

Harris Interactive
2000

eHealth



The WellMed Personal Health Manager delivers sponsor-approved personalized information based on each individual's unique characteristics.

- Comprehensive
- Personalized
- Physician-based

Personally Identifiable Health Information

How do you protect consumer privacy, set proper consumer expectations, build trust, provide connectivity, interactivity and be profitable?

What is the consumer's/patient's expectation of privacy and confidentiality?

“The right to be left alone…”

Louis Brandeis

The right to be left alone is the most comprehensive of rights…”

Olmsted v. United States 1928

Communication Technology 1890:

- Photography
- Cheap Printing

“You already have zero privacy. Get over it.”

Scott G. McNealy

CEO, Sun Microsystems, Inc.

1999

Privacy Protection at Commercial Web Sites

93% of commercial Web sites collect at least one type of personal identification

Less than 10% of sites encompass all five principles:

Notice, Choice, Access, Security, Enforcement

One-third of sites post no privacy policy

Only 19% disclose steps taken to safeguard data

Examples of abuse are widespread

Privacy Rights Clearinghouse
Beth Givens, Director
1999

Privacy Among Top Shopping Sites

- Only a third of surveyed sites guaranteed not to send visitors' personal information to third parties
- 31% of sites have privacy policies that appear to give the owner the right to send personal details to third parties

eMarketer, July 2000 Top 101 Consumer Web sites

Amazon: “Personal info may be shared”

“Dear Customer,

We have just updated Amazon.com's privacy policy and, because privacy is important, we wanted to e-mail you proactively in this case and not just update the policy on our site, as is the common Web practice. Thanks for being a customer and allowing us to continue to earn your trust.

To read the updated Privacy Notice, visit:

http://www.amazon.com/privacy-notice”

Associated Press,
Sep. 1, 2000

The fine print

"As we continue to develop our business, we might sell or buy stores or assets. In such transactions, customer information generally is one of the transferred business assets," the company said. The company also said that "in the unlikely event that Amazon.com Inc., or substantially all of its assets are acquired,customer information will of course be one of the transferred assets."

Consumer Attitudes Mixed

86% favor opt-in privacy policies that require permission for use
54% view Web site tracking of users as invasion of privacy
27% feel that Web site tracking is helpful

54% provided personal information to use a Web site
48% bought online using a credit card
55% sought health information
43% sought financial information
36% went to support-group sites or medical information sites

27% say they will never divulge personal information online

The PEW Internet and American Life Project, 2000

Regulatory Environments

Federal

State

International

Governing Agencies

Industry self regulation

Consumer Expectations

Court of Public Opinion

Fair Information Principles

-provide individuals with a measure of control

HEW(1974):

Openness, Notice, Limitations on secondary use, Correction, Security

OECD(1980):

Purpose specification, Use limitation, Individual participation

FTC(1998):

Notice, Choice, Access, Security, Enforcement

Important Regulations

HHS HIPAA-Health Insurance Portability and Accountability Act of 1996 Proposed HIPPA Regulations

COPPA - Children's Online Privacy Protection Act of 1998 FTC

Gramm-Leach Bliley Act (GLBA)

HIPAA

The purpose is to facilitate the transmission of reasonably identifiable electronic health information data among health payers and providers without compromising the privacy interests of individuals in their health information.

HIPAA Privacy intent:

To provide a floor for national uniformity by preempting only states with weaker privacy protection.

Five key principles of HIPAA

1. **Boundaries:** disclose only for health purposes
2. **Security:** patient authorization for access/legal access
3. **Consumer Control:** person can know and correct contained information
4. **Accountability:** criminal and civil penalties
5. **Public Responsibility:** public health interests preserved

HIPAA Does Not

- Cover all entities that hold individually identifiable health information
- Cover solely paper records
- Provide a statutory authority for a private right of action for individuals to enforce their privacy rights

Does not offer protection for consumer health information

“Individually Identifiable Health Information”

“(6) INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION.—

The term ‘individually identifiable health information’ means any information, including demographic information collected from an individual, that—

Sec. 1171, No. 6, pg. 89

HIPAA, 1996

‘‘(A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

‘‘(B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and—

‘‘(i) identifies the individual; or

‘‘(ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

What happens when covered health information is held by a non-covered entity?

"If a non-covered entity gains access to covered health information, then the information is not covered."

"Chain of trust" applies to information held by covered entity business associates via business contract. The covered entity is responsible."

J. Michael Fitzmaurice – August, 24, 2000

FTC Response to HIPAA

- FTC has interest and authority for consumer protection in this area
- Strongly supports individualized authorization or “opt-in”
- Requests for authorization of use should be specific
- Information practices should be clear and conspicuous

FTC Statutory Authority

Section 5

"Unfair & deceptive acts or practices"

Section 12

"Prohibits the dissemination of misleading claims for food, drugs, devices, cosmetics, or services."

Public Attitudes Toward Medical Privacy

Gallup Survey, Aug. 2000

91% Oppose Medical Identification number

92% Oppose Permitting government agencies to view medical records without explicit permission

93% Oppose permitting researches and scientists to study individual's genetic information without prior consent

95% Feel Doctors and Hospitals should be required to gain patient permission before releasing medical records to a national database

96% Believe personal information told to medical doctors in confidence should not be included in federal computer records.

Children's Online Privacy Protection Act of 1998

Child

An individual under age 13

Collection

Includes direct or passive…"actual knowledge"

Release of Personal Information

"sharing, selling, renting, or any other means of providing personal information to any third party."

Provide Notice

Inform Parents

Obtain Parental Consent

Allow Review

Establishes Rules

Children's Online Privacy Protection Act of 1998

Collected Online

Personally Identifiable Information

- Name
- Physical Address
- Email address or online contact information
- Telephone number
- Social Security number
- Persistent identifier (cookie,etc.)
- Information concerning a child …

Gramm-Leach-Biley (S.900)

Deregulation of Financial Service Organizations

Act pertains to “Customers’ non-public personal information.”

Gramm-Leach-Biley (S.900)

- Accurately, clearly and conspicuously disclose to consumers, at the time relationship is established and not less than annually after that, the organizations' privacy policy for disclosing customers' non-public information
- Provide consumers the right to "opt out" of disclosures of their non-public personal information to non-affiliated third parties (*limited exceptions…)*
- Establish appropriate security and confidentiality measures for customer records and information

wellmed

Representative Leach
Chairman, House Banking and Financial Services Committee

Medical Financial Privacy Protection Act (H.R. 4585)

Goal: Prevent financial institutions from sharing medical financial information without an individual's consent and prohibit the use of medical information in making credit decisions.

The bill requires a specific and separate consent for mental health information, HIV information, genetic information and abortion information.

General Rules for Use of IIHI

Representative Leach
Chairman, House Banking and Financial Services Committee

Medical Financial Privacy Protection Act (H.R. 4585)

- “Opt-in” Consent for health information
- Prohibit disclosure of Information about IIHI - Personal Spending Habits
- Notice and Consent for Aggregate data disclosure to third party
- Exempt use for customer service
- Prohibit re-disclosure and re-use by third parties
- Prohibit requesting of health information from a third party to make a loan or credit decision

California Health Care Foundation

Jan. 2000

- Visitors to health Web sites are not anonymous
- Web site privacy policies fall short of truly safeguarding consumers
- There is inconsistency between privacy policies and actual practices
- Personal health information may not be adequately protected
- Health Web site privacy policies that disclaim liability for actions of third parties negate those very policies

Key Issues

19/21 had privacy policy

Generally lacked notice

Only 8 provided user access to data

Opt out rather than opt in

Third parties

1009 U.S. Adults

CHCF Survey – Public Concern

75% concerned that Web sites have their information without their permission

Significant numbers of people would not engage in online health activities

-40% not give a doctor online record access

-25% not buy or refill Rx online

-16% would not register at sites

17% of people do not go online to seek health information due to their privacy concerns

80% privacy policy with choices had a positive impact on their willingness to engage

Transparency

What relationship is member in?

What rules govern that relationship?

How is member informed?

When is member informed?

“Loss of privacy ranks as a greater concern to US consumers than healthcare, crime or taxes”

Harris Interactive Survey, Oct. 2000

The National Consumers League

Harris Interactive Survey, Oct. 2000
The National Consumers League

- 64% believe websites will share their personal information
- 59% worry websites will collect information without their knowledge
- 91% trust companies to somewhat follow their privacy policies
- 90% have seen a privacy notice

Hi-Ethics Principles

Reliable online information

Responsible online advertising

Private and secure personal health information

- Trustworthy
- Credible
- Reliable

Hi-Ethics
HEALTH INTERNET ETHICS

Hi-Ethics

- A group of major commercial ehealth sites
- Hi-Ethics sites reach more than 30% of Internet audience in general
- More than 60 million visitors have visited Hi-Ethics sites
- Projected 2000 revenues are 2/3 of total eHealth companies[1]

[1]Includes 22 eHealth companies designated by Wit Capital, January 31, 2000

14 Hi-Ethics Principles

1-3	Privacy and Confidentiality
4-6	Advertising and Commerce
7-9	Quality of Health Information
10-11	Best Practices for Professionals
12-14	Disclosure and Feedback

Privacy and Confidentiality

- Must conform with Fair Information Practices
- Protection for Health-Related Personal Information “opt-in”
- Privacy in Relationships with Third Parties
- Provide Customers with Meaningful Choice

Advertising and Commerce

- Disclosure of Ownership and Sponsorship
- Identifying Advertising and “Sponsored” Content
- Promotional Offers, Rebates and Free Items or Services

Hi-Ethics™
HEALTH INTERNET ETHICS

Quality of Health Information

Accuracy and Reliability Editorial Policy

Authorship and Accountability and Date Validation for Self-Help Services

Hi-Ethics™
HEALTH INTERNET ETHICS

Best Practices for Health Care Professionals

- Clarity of Relationships
- Professionalism
- Qualifications

Hi-Ethics CAV

Compliance

Accountability

Verification

Hi-Ethics™
HEALTH INTERNET ETHICS

Combination of Law and Industry Self Regulation

Independent

Multi-Faceted

Multi-Tiered

Independent

- Hi-Ethics will maintain the code and interpretation
- Independent implementation, evaluation and dispute resolution
- Web site does not need to belong to Hi-Ethics to obtain the seal
- Annual Renewal
- Feedback and Monitoring

Hi-Ethics™
HEALTH INTERNET ETHICS

Multi-Faceted

Privacy Audit

Financial Audit

Security Audit

Professionalism compliance

Editorial Policy compliance

Advertising Policy compliance

Evaluation of third party relationships

Hi-Ethics
HEALTH INTERNET ETHICS

No one organization can currently do this all and therefore we are working with three leading organizations to bring forth in January a coordinated “Hi-Ethics Seal” Program

Multi-Tiered

1. Adopt Hi-Ethics Principles
2. Perform Self assessment
3. Publicly announce compliance
4. Independent assessment
5. Voluntary participation in “Hi-Ethics Seal Program”
6. Join Hi-Ethics

Consensus Statement

October 4, 2000

We share the same purpose - to earn the trust of the eHealth consumer.

The three codes were created to address different needs but their underlying principles are compatible.

- **eHealth Ethics Initiative of the Internet Healthcare Coalition**

  Ahmad Risk, MB BCh, Co-chair

- **Health On the Net Foundation (HON)**

  Timothy Nater, Executive Director

- **Health Internet Ethics (Hi-Ethics)**

  Donald W. Kemper, Chairman

Consensus Statement

October 4, 2000

Our respective efforts, once fully implemented, will create a comprehensive system of codes, compliance and verification that will deliver a trustworthy and responsible health Internet.

As the first step, we will create a coordinating committee to establish the common glossary of definitions and terms to be used in our verification and compliance efforts.

We will work to improve and evolve our individual codes and compliance efforts in a coordinated way and will cooperate with other international efforts.

eHealth Code of Ethics: Aspirational Code

- Candor
- Honesty
- Quality
- Informed Consent
- Privacy
- Professionalism in Online Health Care
- Responsible Partnering
- Accountability

HONcode

1. Authority-qualified professional
2. Complementary-support MD/Pt relationship
3. Confidentiality
4. Attribution-data references
5. Justifiability-supportive, balanced evidence
6. Transparency of authorship
7. Transparency of sponsorship
8. Honesty in advertising & editorial policy

AMA Guidelines for Medical and Health Information Sites on the Internet

Guidelines established by the AMA sites, professional sites and for any site displaying AMA's name other than simple link.

Hi-Ethics Collaborative Efforts

- Common set of definitions
- Working with HON and others for European counterpart
- Working with accreditation organizations like NCQA and URAC and IHC in educational efforts
- Recognition of seal equivalents

Our Goal

To build trust so we can reach the full potential of eHealth

wellmed

The key is to set proper customer expectations

…and then to deliver on them.

Making health manageable.

References

IEEE Privacy Statement http://www.ieeeusa.org/forum/POSITIONS/healthinfo.html

Cybercitizen Health Study www.cyberdialogue.com

Children's Online Privacy Protection Rule

http://www.ftc.gov/os/1999/9910/childrensprivacy.pdf

Proposed Standards for Privacy of Individually Identifiable Health Information

Summary: http://aspe.hhs.gov/adminsimp/pvcsumm.htm

Full Reg: http://aspe.os.dhhs.gov/admnsimp/pvctemp.htm

Security and Electronic Signature Standards
http://erm.aspe.hhs.gov/ora_web/plsql/erm_rule.rule_text?user_id=&rule_id=81

WellMed Privacy Statement

www.WELLMED.com/privacy

Privacy and Human Rights

www.epic.org

References

California Healthcare Foundation Privacy Report

http://ehealth.chcf.org

HIPAA

US Health & Human Services on Administrative Simplification -

http://aspe.hhs.gov/admnsimp/

Proposed Standards for Privacy of Individually Identifiable Health Information

Summary: http://aspe.hhs.gov/adminsimp/pvcsumm.htm

Full Reg.: http://aspe.os.dhhs.gov/admnsimp/pvctemp.htm

HIPAAcomply - http://www.hipaacomply.com/

FTC HIPAA Response

Summary http://www.ftc.gov/opa/2000/02/hhsmedpriv.htm

Letter **http://www.ftc.gov/be/v000001.htm**

References

Security and Electronic Signature

Security and Electronic Signature Standards
http://erm.aspe.hhs.gov/ora_web/plsql/erm_rule.rule_text?user_id=&rule_id=81

US Encryption Policy, Jan 14, 2000 http://www.cdt.org/crypto/admin/000114cryptoregs.pdf

HCFA's Internet Security Policy http://www.hcfa.gov/security/isecplcy.htm

HCFA's Internet Policy FAQs *http://www.hcfa.gov/security/fq011399.htm*

State Laws

California senate bills are:

AB 416 Personal information: disclosure.

BILL NUMBER: AB 416 CHAPTERED 09/28/99 CHAPTER 527

SB 19 Medical records: confidentiality.

BILL NUMBER: SB 19 CHAPTERED 09/28/99 CHAPTER 526.

References

Privacy Journal's ranking of states Privacy Protection:
www.townonline.com/privacyjournal

October 1999

"The State of Health Privacy: An Uneven Terrain" Health Privacy Project 7/24/99.
http://www.healthprivacy.org/resources/statereports/preface.html

OECD

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, September 23, 1980, Council of the OECD.
www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.htm

Privacy Protection on Global Networks, OECD Ministerial Conference, Ottawa, October 7-9, 1998. www.oecd.org/dsti/sti/it/secur/act/privnote.htm

Electronic Commerce OECD Policy Brief, No. 1,1997.
www.oecd.org/publications/pol_brief/9701_pol.htm

References

Safe Harbor

Safe Harbor: Draft International Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce http://www.ita.doc.gov/td/econ/Principles1199.htm.

Working Party On the Protection of Individuals with regard to the Processing of Personal Data 5146/99/EN/final Letter Adopted December 3,1999.

March 17, 2000 U.S. Department of Commerce latest Draft http://erm.aspe.hhs.gov/ora_web/plsql/erm_rule.rule_text?user_id=&rule_id=81

References

Global

Privacy & Human Rights 1999. Country Reports.
http://www.privacyinternational.org/survey/

None of Your Business; Peter P. Swire & Robert E. Litan; Brookings Institution Press: 1998.

UK Data Protection Act of 1998; http://www.open.gov.uk.dpr.htm/

Privacy and Human Rights-An International Survey of Privacy Law s and Developments; 1999; Electronic Privacy Information Center and Privacy International; ISBN 1-893044-05-X; www.epic.org

Children's Online Privacy

Children's Online Privacy Protection Rule; 16 C.F.R. Part 132 RIN 3084-AA84; Agency Federal Trade Commission Final Rule ;
http://www.ftc.gov/os/1999/9910/childrensprivacy.pdf

New Rule Will Protect Privacy of Children Online Press Release; FTC
http://www.ftc.gov/opa/1999/9910/childfinal.htm

References

Fair Information Practices

Five Principles http://www.iss.stthomas.edu/lc/fair_information_practices.htm

Code of Fair Information Practices
http://www.epic.org/privacy/consumer/code_fair_info.htm

Privacy Act of 1974 Law ftp://ftp.cpsr.org/cpsr/privacy/law/privacy_act_1974.txt

The citation for the report is as follows: U.S. Dep't. Of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens viii (1973).

WellMed Privacy Statement http://www.wellmed.com/wellmed/aboutus/privacy.html

Other Sources

Tunitas Group - http://www.tunitas.com/

Health Privacy Project - http://www.healthprivacy.org/

Arthur Anderson - http://ww3.knowledgespace.com/Healthcare/

References

WEDI - http://www.wedi.org/

AHIMA - http://www.ahima.org/

Washington Publishing Company - http://www.wpc-edi.com/HIPAA_40.asp

IEEEPrivacy Position Paper - http://www.ieeeusa.org/forum/POSITIONS/healthinfo.html

Cybercitizen Health Study - www.cyberdialogue.com

FTC Advisory Committee on Online Access and Security - http://www.ftc.gov/acoas/

Hi-Ethics - www.hiethics.com

eHealth Ethics Code- www.ihealthcoalition.org/ethics.html

AMA Web Guidelines- http://www.ama-assn.org/about/guidelines.htm