HIPAA Privacy Compliance for E-Health Sites

Michael Rozen, MD
Chief Privacy Officer
VP, Consumer Affairs
WellMed, Inc.

wellmed

Howard Bell
Writer,
Healthcase
Informatics
Feb, 2000

"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."

wellmed

eHealth

Non Traditional Stakeholders

Connectivity

Data Empowerment

Interactivity

Up close and personal

wellmed

Consumer-Centric Health Management

wellmed

eCare

- Traditional stakeholders
- Using electronic medium to deliver care
- 32 % Employers using Internet to Administer health benefits

Evolving Issues

- Data Interchange
- Messaging
- Email
- Ubiquitous Wireless Connectivity
- Decision Making Support
- Data Interpretation
- Closing the Loop to Physician Desktop
- Consumer Claims-Processing Support

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?

Privacy

“It is a riddle wrapped in a mystery inside an enigma”

Winston Churchill
Russia

“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

wellmed

"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

One third of sites post no privacy policy

Only 19% disclose steps taken to safeguard data

Examples of abuse are widespread

Five Principles for Privacy Protection:

Notice, Choice, Access, Security, Enforcement

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 appears to give owner the right to send personal details to third parties

eMarketer, July 2000
Top 101 Consumer Websites

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”

wellmed

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

86 % favor opt-in privacy policies that require permission for use

54 % view website tracking of users as invasion of privacy

Only 27 % feel that website tracking is helpful

54% have provided personal information to use a Web site.

48% have bought online using a credit card

55 % have sought health information

43 % have sought financial information

36 % went to support-group sites or medical information sites

27 % say they will never divulge personal information online

Medical Record Privacy Concerns

78% of Doctors withhold information from patient record due to privacy concerns

87% of Doctors reported having had a patient request to withhold information from their records

Association of American Physician and Surgeons

Regulatory Environments

Federal

State

International

Governing Agencies

Industry self regulation

Consumer Expectations

Court of Public Opinion

Sectoral Laws

Unleveled playing field

“Safe Harbor”

HHS, FTC, FDA, SEC…

Hi Ethics, OPA

Fair Information Practices

1965 House of Representatives Subcommittee

1973 HEW "The Code of Fair Information Practice Principles"

1974 Federal Privacy Act

- Notice (awareness)
- Choice
- Access
- Security
- Data Integrity

1998 FTC defacto standards for privacy protection on the Internet

Important Regulations

- COPPA-Children's Online Privacy Protection Act of 1998 FTC
- HIPAA-Health Insurance Portability and Accountability Act of 1996
- Gramm-Leach Bliley Act (GLBA)

Children's Online Privacy Protection Act of 1998

Child-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

"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

HIPAA Privacy History

Aug. 21, 1996	HIPAA, Public Law 104-109
Aug. 21, 1999	Congressional Deadline
Oct. 29, 1999	HHS Draft Issued
Nov. 3, 1999	64 FR 59918
Feb.17, 2000	End comment Period
Dec. 20, 2000	HHS Final Privacy Rule
Dec. 28, 2000	65 FR 82462
Feb.26, 2003	Compliance Date (2004 smaller plans)

Purpose of Administrative Simplification Privacy Regulations

1. Protect and enhance consumer rights:
   - access to their information
   - controlling inappropriate use
2. Improve quality by restoring trust
3. Improve efficiency and effectiveness by creating national framework for health privacy protection

HIPAA Privacy Overview

- Establishes a set of basic national privacy standards
- Sets a floor for privacy ground rules
- Seeks to balance need of individual with needs of society
- “Privacy is a fundamental right”

Components of Final Privacy Rule

- Consumer control over Health Information
- Boundaries on Medical Record Use and Release
- Ensure Security of Personal Health Information
- Establish Accountability for Medical Record Use and Release
- Balance Public Responsibility with Privacy Protections
- Special Protection for Psychotherapy Notes

Changes from Proposed Regulation

- Provide coverage to all individually identifiable health information held by a covered entity
- Requires consent for routine use and disclosure - Health providers obtain general consent for treatment, payment and health care operations accompanied with detailed notice
- Allows disclosure of full medical record for treatment
- Protects against unauthorized use of medical records for employment purposes

Changes from Proposed Regulation

- Enforcement – OCR
- "Business associate"
- Clearinghouses are not subject to certain requirements in the rule when acting as business associates of other covered entities.
- Minors-federal privacy right attached to consent for treatment right
- Marketing and fund raising use of information

Covered Information

In final rule, scope of protection extended to all individually identifiable health information in any form, electronic or non-electronic, held or transmitted by a covered entity.

Consent

- Covered health care providers who have a direct treatment relationship with an individual are required to obtain a general consent from the individual in order to use or disclose the protected health information for treatment, payment and health care operations.
- Providers may condition treatment on patient's providing consent.
- For psychotherapy notes, for most purposes, an individuals authorization is required.

Authorization

- Required for all disclosures and uses not expressly exempted in the regulation.
- Can not condition services or payment on receipt of authorization

Marketing (authorization required)

Communication about a product or service a purpose of which is to encourage recipients to purchase or use the product or service

Three exceptions:

-Marketing the organization

-Part treatment or health of individual

-In the course of managing the treatment of individual or directing to recommending other treatments, etc.

Notice

"THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY"

Covered entities must describes all uses and disclosures of protected health information they are permitted or required to make without authorization including those uses and disclosures under consent requirements.

Notice

Additionally, covered entities have to disclose those activities where they may want to contact the individual

-providing appointment reminders

-describing/recommending treatments

-providing health benefit information

-soliciting funds

Direct treatment providers must provide notice at time of first service delivery either in person or electronically. Under final rule, a covered entity that maintains a web site describing the services and benefits it offers must make its privacy notice prominently available through the site. Individual has

Data Interchange

For release of personally identifiable information, the user must explicitly authorize such release. The authorization must state:

- Purpose for release
- Information to be shared
- Who information shared with
- Duration of authorization
- Provide user opportunity to revoke authorization at any time

What is Medical Record?

No accepted standard definition

What is Health Information?

The Health Insurance Portability and Accountability Act of Aug, 1996. HR 3103, PL 104-191.

‘‘(4) HEALTH INFORMATION.—The term ‘health information means any information, whether oral or recorded in any form or medium, that—

‘‘(A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, 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.”

"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—

''(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 is a Personal (Consumer) Health Record?

ASTM Subcommittee
Consumer Health Record

An electronic application where individuals can maintain and manage their health information and that of others for whom they are authorized in a private, secure, and confidential environment that allows the individual or other authorized persons to access and share such information.

Designated Record Set

- Certain records maintained by or for a covered entity that are always part of a covered entity's designated record sets and to include other records that are used to make decisions about individuals.
- The means of retrieval of a record is not a defining criteria.

Creation of De-identified Information

164.502(d) permits a covered entity to use protected information to create de-identified information, whether or not the de-identified information is to be used by the covered entity. It is not subject to privacy rules unless re-identified.

wellmed

Aggregate Data
vs.
Personally Identifiable Information

"Who owns the data?"

"Who has a right to the data?"

Employers

- Not covered entities under the privacy regulation
- Are subject to federal disability nondiscrimination laws
  - ADA, 42 U.S.C. 12111-15 or more employees
  - Governs transmission to covered entity
  - Can use medical information for insurance purposes

Clinical Laboratories

CLIA, 42 U.S.C. 263a and reg 42 CFR part 493

- Require clinical labs to disclose test results/reports only to authorized persons as defined by State Law. Federal law defines it as the person who orders the test. Under this law, a clinical lab may be prohibited from providing the individual who is the subject of the test result access to this information. Under HIPAA, then the lab is exempted from reporting the result to the patient.
- If the clinical lab operates in a state in which the term authorized person is defined to include the individual, then the lab would have to provide the individual with these rights.
- Similarly, research labs that do not report patient specific results for diagnosis prevention or treatment are exempted from providing patient access under HIPAA.

wellmed

Patients/consumers are not covered entities and therefore HIPPA does not offer privacy protection to the individually identifiable health information they maintain/hold about themselves or their family.

EU Safe Harbor

"We believe they are essentially consistent and that an organization complying with our privacy regulation can fairly and correctly self-certify that it complies with the Principles."

Questions regarding compliance and interpretation will be decided based on U.S. Law

U.S.
"Safe Harbor Principles"

Notice	Informed Consent
Choice	"Opt-out"
Sensitive	"Opt-in"
Onward Transfer	Third Parties
Security Protection	"Reasonable
Data Integrity	Accurate, current
Access	Unconditional v Reasonable
Enforcement	Recourse & Penalty

Gramm-Leach-Bliley (S.900)

-Deregulation of Financial Service Organizations

-Act pertains to “Customers’ nonpublic personal information.”

Gramm-Leach-Bliley (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 the Consumer the right to "opt out" of disclosures of their nonpublic personal information to non-affiliated third parites (*limited exceptions...)*

-Establish appropriate security and confidentiality measures for customer records and information

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.

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

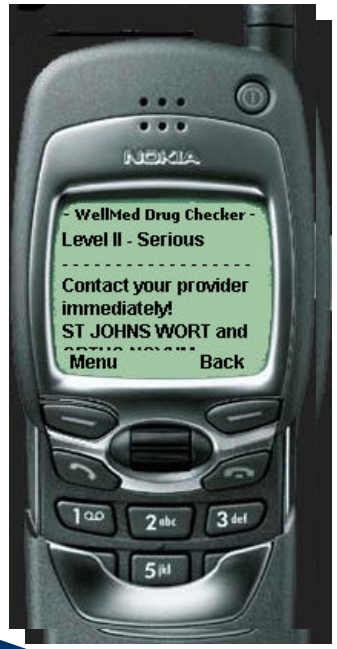
-Exempt use for customer service

-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

wellmed

Customized Connectivity



Tailored Communication

- Deliver personalized content, tailored advertising, relevant information
- Personal Health Manager Home Page
- Tailored email
- Secure instant messaging
- Targeted ecommerce
- Access and pre-qualification to appropriate clinical trials

Problem: Content of the electronic message may allow an individual to be associated with their unique health characteristics and thus their privacy violated

Email and Messaging

WellMed's Philosophy

Push	Wellness (Opt-out)
Pull	Disease (Opt-in)
Secure	The Unmentionable

wellmed

The Prime Directive

The actions of an eHealth or eCare Web site do not allow an individual to be identified with their unique health characteristics without the individual's opt-in authorization.

Hi-Ethics Principles

- Reliable online information
- Responsible online advertising
- Private and secure personal health information

Hi-Ethics
HEALTH INTERNET 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

Hi-Ethics™
HEALTH INTERNET ETHICS

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

Hi-Ethics™
HEALTH INTERNET ETHICS

Advertising and Commerce

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

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 Healthcare Professionals

Clarity of Relationships

Professionalism

Qualifications

Hi-Ethics™
HEALTH INTERNET ETHICS

Combination of Law and Industry Self Regulation

Independent

Multi Faceted

Multi Tiered

CAV Program

- Truste will administer Independent implementation, evaluation and dispute resolution
- Hi Ethics will maintain the code and interpretation
- 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

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

wellmed

eHealth Site Privacy Policy

Disclosure

Authorization

In Summary

- Migration of eHealth to eCare
- Rapid explosion of communication technologies
- Background of conflicting sectoral laws and regulations exist
- Issues extend beyond privacy and security
- Difficult to legislate ethical behavior and morality
- **Blend of Industry Self-regulation augmented with legislation offers enhanced consumer protection**

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

Department of Commerce: Elements of Effective Self Regulation for the Protection of Privacy and Questions Related to Online Privacy.
http://www.ntia.doc.gov/ntiahome/privacy/6_5_98fedreg.htm

Institute for Health Care Research and Policy -Georgetown University:
www.healthprifvacy.org

Final Rule: Privacy Standards. http://aspe.hhs.gov/admnsimp/