COALITION FOR PATIENT PRIVACY

June 26, 2009

Office of the National Coordinator for Health Information Technology
200 Independence Ave, SW
Suite 729D
Washington, DC 20201
Attention: HIT Policy Committee Meaningful Use Comments

Also Submitted via email to MeaningfulUse@hhs.gov

The Coalition for Patient Privacy is a diverse, bipartisan group of organizations that represents millions of Americans. We promote health IT that strengthens consumer control over protected health information so that the United States' electronic health system will be trusted and used by patients. Consumer control also ensures that the data available for research is accurate and complete, rather than the inaccurate and incomplete data we have today on all sensitive or stigmatized illnesses.

We envision an ethical health system that reaps the benefits of technology while simultaneously protecting our children and grandchildren from discrimination based on their protected health information. Individuals can best ensure that personal data goes *only* to the 'right' places at the 'right' time. With control over PHI, consumers can prevent the most egregious violations of privacy and most destructive uses of our health information, including rampant electronic fraud and identity theft by limiting who can access our records.

The KEY CRITICAL FUNCTION needed in every EHR to enable "meaningful use" of EHR data is the ability for patients to control the uses and disclosures of all protected health information (PHI). We recommend adopting existing open source technology that enables detailed control over disclosures as a baseline model or floor for consent technologies. The millions of members in our organizations want granular control over disclosures of their electronic health records, analogous to the ethical principles that have long governed our control over disclosures from paper health records.

The Meaningful Use Workgroup recommended to the Health IT Policy Committee that proposed "meaningful use" functions in EHRs should be "ultimately ***linked to achieving measurable outcomes*** in patient engagement, care coordination, and population health."

We believe that only if patients are willing to participate in the healthcare system and trust doctors with their most sensitive concerns will they disclose complete and accurate information necessary to achieve measurable and reliable outcomes.

Accurate and complete information cannot be obtained by force. We know from the California HealthCare Foundation's National Consumer Health Privacy Survey of November 9, 2005 that 1/8 patients or 12.5% of the population avoids their regular doctor, asks doctors to alter diagnoses, pays privately for a test, or avoids test altogether. If we do not restore patient control over PHI, we can expect electronic health data to have error and omission rates of up to 12.5 %. The breakthroughs and benefits possible with technology-enhanced research will never be reached with such a high rate of errors and omissions.

- Absent and erroneous data = garbage in
- Garbage in = garbage out

- Garbage out = faulty research
- **Research using bad data won't produce reliable outcomes measures or generate answers about "comparative effectiveness". When so many patients get treatment off-the grid or avoid treatment altogether, no data is produced.**

See CHCF survey at: http://www.chcf.org/topics/view.cfm?itemID=115694

The Workgroup recommended 5 policy priorities, with goals and objectives to be achieved between 2011 and 2015, and methods to measure those achievements. The policy priorities are (1) improve quality, safety, efficiency, and reduce health disparities, (2) engage patients and families, (3) improve care coordination, (4) improve population and public health, and (5) ensure adequate privacy and security protections for personal health information.

Our recommendations focus on the Workgroup's Policy priority (5), because none of the *other* policy priorities can be achieved unless the public trusts doctors and consumer control over PHI is restored.

The Coalition's key recommendation to ensure "adequate privacy and security protections for personal health information" is to restore consumer control over PHI in electronic health records and systems. America will never get the data most needed for critical kinds of research like comparative effectiveness, P4P, quality improvement, population health, personalized medicine, and genetic research unless patients are certain that their sensitive health records will not be used without informed consent. Research ethics are based on informed consent for participation, which follow from the Hippocratic Oath requiring patient consent before secrets are shared.

Recommendations:

1) The Coalition for Patient Privacy recommends using the consent requirements in the existing federal regulation 42 CFR Part 2 for the release of information relating to alcohol and substance abuse be used as the policy standard for the release of all protected health information.

See Title 42: Public Health, PART 2—CONFIDENTIALITY OF ALCOHOL AND DRUG ABUSE PATIENT RECORDS, Subpart C—Disclosures With Patient's Consent at http://ecfr.gpoaccess.gov/cgi/t/text/textidx?c=ecfr&sid=fcebf9c9cc10f7fe148f6c1d2f0f5753&rgn=div8&view=text&node=42:1.0.1.1.2.3.1.1&idno=42. See addendum to this document.)

The detailed consent provisions in this federal statute have been implemented very successfully by behavioral treatment centers that are members of the National Data Information Infrastructure Consortium (NDIIC). Electronic consent is used in over 22 regions in 8 states, for the disclosure of records of 4 million patients over the past 9 years. The NDIIC electronic consents include all consent elements in 42 CR Part 2, including the Prohibition on redisclsosure, successfully enabling the electronic exchange of this highly sensitive data for years at low cost. See: http://ecfr.gpoaccess.gov/cgi/t/text/textidx?c=ecfr&sid=fcebf9c9cc10f7fe148f6c1d2f0f5753&rgn=div8&view=text&node=42:1.0.1.1.2.3.1.2&idno=42

Because these electronic consents are open source, they can easily be adapted and validated by the NDIIC and other communities that validate open source technologies. At the same time, 42 CFR Part 2

allows for disclosures in medical emergencies, research activities, and audit and evaluation activities. See: http://ecfr.gpoaccess.gov/cgi/t/text/textidx?c=ecfr&sid=42bbb5435b731dae7ede9379cc97f76e&rgn=div6&view=text&node=42:1.0.1.1.2.4&idno=42

2) The Coalition for Patient Privacy recommends using the electronic open source consents developed by the NDIIC that meet the requirements of 42 CFR Part 2 for the release of information relating to alcohol and substance abuse be used as the minimum standard for electronic consent to release of all protected health information. See: http://www.ndiic.com/ and contact http://www.ndiic.com/staff.shtml for further information on electronic consent modules.

Sincerely:

The Coalition for Patient Privacy

American Civil Liberties Union
Consumer Action
Electronic Frontier Foundation
Just Health
The Multiracial Activist
The National Coalition of Mental Health Professionals and Consumers
Patient Privacy Rights
Private Citizen, Inc.
United States Bill of Rights Foundation

Addendum: 42 CFR Part 2 "Form of written consent".

(a) *Required elements.* A written consent to a disclosure under these regulations must include:

(1) The specific name or general designation of the program or person permitted to make the disclosure.

(2) The name or title of the individual or the name of the organization to which disclosure is to be made.

(3) The name of the patient.

(4) The purpose of the disclosure.

(5) How much and what kind of information is to be disclosed.

(6) The signature of the patient and, when required for a patient who is a minor, the signature of a person authorized to give consent under §2.14; or, when required for a patient who is incompetent or deceased, the signature of a person authorized to sign under §2.15 in lieu of the patient.

(7) The date on which the consent is signed.

(8) A statement that the consent is subject to revocation at any time except to the extent that the program or person which is to make the disclosure has already acted in reliance on it. Acting in reliance includes the provision of treatment services in reliance on a valid consent to disclose information to a third party payer.

(9) The date, event, or condition upon which the consent will expire if not revoked before. This date, event, or condition must insure that the consent will last no longer than reasonably necessary to serve the purpose for which it is given.

(b) *Sample consent form.* The following form complies with paragraph (a) of this section, but other elements may be added.

1. I (name of patient) o Request o Authorize:

2. (name or general designation of program which is to make the disclosure)

_____

3. To disclose: (kind and amount of information to be disclosed)

_____

4. To: (name or title of the person or organization to which disclosure is to be made)

_____

5. For (purpose of the disclosure)

_____

6. Date (on which this consent is signed)

_____

7. Signature of patient

_____

8. Signature of parent or guardian (where required)

_____

9. Signature of person authorized to sign in lieu of the patient (where required)

_____

10. This consent is subject to revocation at any time except to the extent that the program which is to make the disclosure has already taken action in reliance on it. If not previously revoked, this consent will terminate upon: (specific date, event, or condition)

(c) *Expired, deficient, or false consent.* A disclosure may not be made on the basis of a consent which:

(1) Has expired;

(2) On its face substantially fails to conform to any of the requirements set forth in paragraph (a) of this section;

(3) Is known to have been revoked; or

(4) Is known, or through a reasonable effort could be known, by the person holding the records to be materially false.

Preserving The Patient's Right To Health Information Privacy Is Essential For Quality Mental Health Care And Public Acceptance Of A National Electronic Health Information System

American Psychoanalytic Association
American Association of Practicing Psychiatrists

February 22, 2010

THE IMPORTANCE OF RECOGNIZING AND PRESERVING THE RIGHT TO PRIVACY IN A NATIONAL ELECTRONIC HEALTH INFORMATION SYSTEM

Briefing of Dr. David Blumenthal, National Coordinator
for Health Information Technology

February 22, 2010

American Psychoanalytic Association and
American Association of Practicing Psychiatrists

I. The Importance Of The Right To Privacy In Quality Health Care And Effective Psychotherapy.

A. HHS findings under Secretary Shalala—Health information privacy "is necessary to secure effective, high quality health care" because the "entire health care system is built upon the willingness of individuals to share the most intimate details of their lives with their health care provider."[1]

B. U.S. Supreme Court findings—Based on the "reason and experience" of the nation, "[e]ffective psychotherapy, by contrast [with treatment for physical ailments] depends upon an atmosphere of confidence and trust in which the patient is willing to make a frank and complete disclosure of facts, emotions, memories, and fears. . . . For this reason, the mere possibility of disclosure of confidential communications made during counseling sessions may cause embarrassment or disgrace."[2]

[1] HHS finding, 65 Fed. Reg. at 82,467 (Dec. 28, 2000).
[2] Jaffee v. Redmond, 116 S. Ct. 1923, 1928 (1996).

II. Preservation Of The Right To Privacy Is Essential For Quality Health Care.

A. Each year more than 2 million Americans do not seek treatment for mental illness due to privacy fears.[3]

B. 150,000 war veterans returning from Iraq and Afghanistan suffering from Post-Traumatic Stress Disorder did not seek treatment due to privacy concerns.[4]

C. Many Americans believe their personal health information is at risk of being improperly disclosed in an electronic information system. A recent survey showed that 59% of Americans "were not too confident or not confident at all that their electronic [health] records would remain confidential, and 76% believed it would be very or somewhat likely that an unauthorized person would be able to access their medical record."[5]

D. Patients who are worried about the possible misuse of their health information will protect their privacy by avoiding or delaying health care, paying out of pocket, changing physicians or asking physicians to not record information or misrepresent it in the record."[6]

1. If the privacy of conversations between psychotherapists and patients were not protected, those confidential conversations "would surely be chilled."[7]

2. If privacy concerns are not addressed, these concerns may result in mental health patients "limiting their revelations, and altering the accuracy of events and feelings they disclose to their mental health providers."[8]

---

[3] HHS finding, 65 Fed. Reg. at 82,779.
[4] "Invisible Wounds of War," The RAND Corp., p. 436 (2008).
[5] "Openness of Patients' Reporting with Use of Electronic Records: Psychiatric Clinicians' Views," Journal of American Informatics Association, p. 54 (2009).
[6] HHS Finding, 65 Fed. Reg. at 82,468; "Openness of Patients' Reporting with Use of Electronic Records: Psychiatric Clinicians' Views," p. 55.
[7] Supreme Court finding, Jaffee v. Redmond, 116 S. Ct. at 1929.
[8] "Openness of Patients' Reporting with the Use of Electronic Records," p. 55.

3. In recent surveys of mental health professionals that use an electronic health information system at a major university medical system:

   a. 98% reported that confidentiality of psychiatric records is important to their professional work;
   b. 94% reported that confidentiality of psychiatric records is important to them and their immediate family's records;
   c. 63% reported electronic health records lessened their willingness to record highly confidential information;
   d. 70% reported that concerns with the confidentiality of electronic medical records caused them to use more "measured (selective, discrete) wording in the medical record;"
   e. 60% reported that because of concerns with the confidentiality of electronic medical records they are more concerned that non-mental health providers will misunderstand information in the record; and
   f. Only 4% reported that electronic records increased patients' willingness to divulge confidential information.

E. Since January 2005, the privacy of more than 45 million electronic health records has been reported breached.[9]

F. The actual number of electronic health records breached or compromised could be double given that nearly half of breaches go unreported.[10]

[9] See Tab 3.
[10] "Nearly Half of Data Breaches Not Disclosed: Report," Modern Healthcare Online (April 8, 2008).

G. Congress, the Government Accountability Office (GAO), and HHS have all concluded that the increasing use of electronic information systems "has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information."[11]

H. Electronic data breaches appear to be increasing, and it does not appear that these systems can be made secure.[12] In fact, "there is no such thing as a totally secure [HIT] system that carries no risk to security."[13]

I. The adverse consequences of an electronic privacy breach are greater because, <u>for the first time in the history of medicine</u>,

1. Identifiable health information of millions of individuals can be improperly disclosed to millions of other individuals "in a matter of seconds;"[14]

2. Health information may be stolen by individuals who do not have physical access to the records and who may not even reside in the United States;[15] and

---

[11] Congressional Finding, Pub. L. 93-579, section 2(2); "Cyber Security: A Crisis in Prioritization," President's Information Technology Committee, p. 5 (Feb. 28, 2005) ("The IT Infrastructure of the United States is highly vulnerable to terrorist and criminal attacks."); "Health Information Technology: Early Efforts Initiated But Comprehensive Privacy Approach Needed for National Strategy," GAO-07-238, p. 27 (Jan. 10, 2007) ("[T]he increased risk of inappropriate access and disclosure raises the level of importance for adequate privacy protections and security mechanisms to be implemented in health information exchange systems."); HHS finding: "The electronic information revolution is transforming the recording of health information so that the disclosure of information may require only a push of a button. In a matter of seconds, a person's most profoundly private information can be shared with hundreds thousands, even millions of individuals and organizations at a time." 65 Fed. Reg. at 82,465.

[12] "Data Breaches Up Almost Fifty Percent, Affecting Records of 35.7 Million People," The Washington Post (Jan. 6, 2009); "In Cyber War Age, U.S. Finds No Easy Deterrent," The New York Times (Jan. 26, 2010); "Electronic Health Records Could Be A Deadly Target During a Cyberwar," Nextgov: Technology and the Business of Government (Nov. 20, 2009).

[13] HHS Finding, 68 Fed. Reg. at 8,346 (Feb. 20, 2003).

[14] HHS Finding, 65 Fed. Reg. at 82,465; "An Ominous Milestone: 100 Million Data Leaks," The New York Times (Dec. 18, 2006); "Vast Data Cache About Veterans is Stolen," The New York Times (May 23, 2006); "Veterans Administration Loses Data," Consumer Affairs Feb. 18, 2007); "Medicare and Medicaid Gaps Are Found," The New York Times (Oct. 21, 2006).

3. When an individual's health information privacy is breached electronically, it can never be restored.[16]

III. Preservation Of The Patient's Right To Privacy Is Essential For The Successful Implementation Of A National Electronic Health Information System.

A. "[P]ublic support for the NHIN depends on public confidence and trust that personal health information is protected. Any system of personal health information collection, storage, retrieval, use, and dissemination requires the utmost trust of the public."[17]

B. One of the biggest challenges of implementing an electronic health information system "will be maintaining the trust of the public."[18]

IV. The Right To Health Information Privacy Has Been Recognized By All Three Branches Of The Federal Government And By All 50 States.

A. Congressional finding—Americans have a right to privacy for personal information that is a "personal and fundamental right protected by the Constitution of the United States."[19]

B. HHS finding—"Privacy is a fundamental right. . . . A right to privacy in personal information has historically found expression in American law."[20]

---

[15] "Experts: Medical Identity Theft Growing, Tough to Detect," Philadelphia Business Journal (Oct. 19, 2007); "Breaking the Code: How Credit-Card Data Went Out Wireless Door," Wall Street Journal (May 4, 2007); "Medical Identity Theft is a Growing Problem," The Heartland Institute (Sept. 2007).

[16] HHS Finding, 65 Fed. Reg. at 82,465.

[17] Finding by National Committee on Vital and Health Statistics, letter to HHS Secretary Leavitt (June 22, 2006).

[18] Statement of Dr. David Blumenthal, National Coordinator for Health Information Technology, "Connecticut AG Sues Health Net Over Security Breach," Government Health IT News (Jan. 14, 2010).

[19] Congressional Finding, The Privacy Act, Pub. L. 93-579, section 2(a)(4).

[20] 65 Fed. Reg. at 82,464.

C. Supreme Court finding—The right to privacy of highly personal information is protected by the Fourth and Fifth Amendments to the United States Constitution.[21]

D. "Federal common law and the law of all 50 states and the District of Columbia recognize the patient's right to privacy under the psychotherapist-patient privilege.[22]

E. "All fifty states today recognize in tort law a common law or statutory right to privacy."[23]

F. Ten states recognize a right to privacy in state constitutions.[24]

G. The right to health information privacy and consent is recognized in the minimum standards for the ethical practice of medicine and psychotherapy.[25]

1. The standards of ethics for psychoanalysts provide:

a. Confidentiality. Confidentiality of the patient's communications is a basic patient's right and an essential condition for effective psychoanalytic treatment and research.[26]

---

[21] Ferguson v. City of Charleston, 532 U.S. 67 (2001); Whalen v. Roe, 429 U.S. 589 (1977); U.S. v. Scott, 424 F.3d 888 (9th Cir. 2005); Douglas v. Dobbs, 419 F.3d 1097 (10th Cir. 2005); Tucson Woman's Clinic v. Eden, 371 F.3d 1173 (9th Cir. 2004).

[22] Jaffee v. Redmond, 116 S. Ct. at 1928-1929.

[23] HHS Finding, 65 Fed. Reg. at 82,464.

[24] Those states are Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington. Other states, like Texas and Tennessee, have a right to privacy for personal information implied in their constitutions.

[25] Finding of the National Committee on Vital and Health Statistics, letter to Secretary Leavitt (June 22, 2006).

[26] See "Principles and Standards of Ethics for Psychoanalysts," American Psychoanalytic Association (2009-2010).

V. Essential Elements For Protecting The Patient's Right To Health Information Privacy And Access To Quality Psychotherapy.

A. Recognize that individuals *have* a right to health information privacy that will be preserved and protected in an electronic health information system.

1. HHS recognized in the preamble to the Original HIPAA Privacy Rule that individuals have a right to health information privacy, but failed to include a right to privacy among the rights protected by the HIPAA Privacy Rule.[27]

2. A right to health information privacy is not currently one of the patient rights included in the HIPAA notice of privacy practices, nor is it included among the rights listed on the OCR website.[28]

B. Adopt the commonly accepted definition of "health information privacy."

1. The National Committee of Vital and Health Statistics found, after 18 months of hearings and research, that, "Health information privacy is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data."[29]

2. HHS has found that "the right to privacy is 'the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated.'"[30]

---

[27] 45 C.F.R. 164.520(b)(1)(iv) listing "individuals rights" as the right to (a) request restrictions, (b) receive confidential communications, (c) inspect and copy PHI, (d) amend PHI, (e) receive an accounting of disclosures, and (f) obtain a paper copy of the notice of privacy practices.

[28] See "What Rights Does the Privacy Rule Give Me Over My Health Information?" http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html.

[29] NCVHS Finding, letter to Secretary Leavitt (June 22, 2006).

[30] HHS Finding, 65 Fed. Reg. at 82,465.

3. Federal courts have routinely defined the right to informational privacy as "control over knowledge about one's self."[31] The most often quoted definition is that privacy is "the right to be let alone."[32]

C. Expressly preserve the patient's right to privacy under the psychotherapist-patient privilege and include this in the notice of rights to patients.

1. The HITECH Act, at section 13421(c) expressly acknowledged the existence of privileges and the intent of Congress that nothing in the health information privacy legislation is intended to "constitute a waiver of any privilege."

2. The notice of privacy practices should inform patients that the psychotherapist-patient privilege can be waived only by them.

3. In recognizing and preserving the psychotherapist-patient privilege, there should be no "balancing" of the patient's interest against society's interest because "[a]n uncertain privilege, or one which purports to be certain but results in widely varying applications . . . is little better than no privilege at all." The psychotherapist-patient privilege furthers both the public's and the individual's interest in access to effective psychotherapy.[33]

[31] U.S. v. Westinghouse, 638 F.2d 570, 577, n. 5 (3rd Cir. 1980).
[32] "The Right to Privacy," L. Brandeis and S. Warren, 4 Harv. L. Rev. 193 (1890).
[33] Supreme Court holding, Jaffee v. Redmond, 116 S. Ct. at 1929.

D. Include the patient's right of authorization for disclosure of "psychotherapy notes" in the notice of privacy practices.

1. The HIPAA Privacy Rule provides that "psychotherapy notes" may not be used or disclosed, with few exceptions, without the patient's authorization, but this important privacy right is not included in the rights that must be included in the notice of privacy practices.[34]

E. Allow for the "segmentation and protection from disclosure" of sensitive identifiable mental health information "with the goal of minimizing the reluctance of patients to seek care (or disclose information about a condition) because of privacy concerns."

1. This is a required consideration by the HIT Policy Committee under the HITECH Act in section 3002(b)(2)(B).

2. A psychiatric department in a major university medical center has adopted an electronic health information system in which "all notes, appointments, and phone communications were sequestered in a separate database accessible only to psychiatric clinicians and staff."[35]

F. Clearly state in regulations that "minimum necessary" determinations are to be "consistent with, and not override, professional judgment and standards."

1. The preamble to the Original and Amended HIPAA Privacy Rule have both stated that minimum necessary determinations are "intended to be consistent with, and not override professional judgment and standards."[36]

---

[34] Compare 45 C.F.R. § 164.508(a)(2) with 164.520(b)(1)(iv).
[35] "Openness of Patients' Reporting with Use of Electronic Records," p. 55.
[36] HHS interpretation, 67 Fed. Reg. at 53,197 and 65 Fed. Reg. at 82,544 (The 'minimum necessary' standard is intended to reflect and be consistent with, not override, professional judgment and standards.")

2. The HITECH Act at section 13405(b)(2) provides that the covered entity or business associate disclosing the information shall determine what constitutes the minimum necessary information to accomplish the intended purpose of the disclosure.

3. Mental health professionals must be allowed to adhere to their ethical standards in making "minimum necessary" determinations.

G. The patient's right to pay privately to protect the privacy of mental health information must be preserved.

1. Patients have always enjoyed a right to pay privately and not have their identifiable health information disclosed without their permission.

2. The HITECH Act, section 13405(a) confers a new right on patients to have covered entities not disclose identifiable health information to a health plan for payment or health care operations purposes if the patient pays out of pocket in full.

3. This right should be included in the notice of privacy practices made available to patients.

Tab 1

The Right to Health Information Privacy

February 10, 2010

James C. Pyles
Powers, Pyles, Sutter & Verville, P.C.
1501 M Street
Washington, D.C. 20005
(202) 466-6550
jim.pyles@ppsv.com

Congress has previously found that Americans have a right to privacy for personal information about themselves that is a "personal and fundamental right protected by the Constitution of the United States."[1] The federal courts and the Department of Health and Human Services have recognized that the right to privacy has two branches. One branch is "the individual interest in avoiding disclosure of personal matters" (informational privacy) and the other is "the interest in independence in making certain kinds of important decisions" (decisional privacy).[2]

Prevailing federal case law provides that "[t]here can be no question that an [individual's] medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection...[defined as]...control over the knowledge about oneself."[3] The right to informational privacy is "one of the most cherished rights of American citizenship commonly characterized as the right to be let alone."[4] Medical records and information "stand on a different plain than other relevant materials" and are generally afforded a higher level of privacy protection.[5] If there is no right to privacy for one's health information, which may include information on a person's genetic make-up and inner-most thoughts, a right to privacy might not exist for any information.[6]

Federal courts have found that the constitutionally protected right to privacy of highly personal information, including health information, has become so well established that no reasonable government employee

---

[1] Pub. L. 93-579, section 2(a)(4).
[2] Whalen v. Roe, 97 S. Ct. 869, 876 (1977); finding by the Department of Health and Human Services, 65 Fed. Reg. at 82,464 (Dec. 28, 2000).
[3] United States v. Westinghouse, 638 F.2d 570, 577, n.5 (3rd Cir.1980).
[4] United States v. Westinghouse, 638 F.2d at 576; *see also* HHS finding, 65 Fed. Reg. at 82,464.
[5] United States v. Westinghouse, 638 F. 2d at 577.
[6] HHS Findings, 65 Fed. Reg. at 82,464, 82,466.

could be unaware of it.[7] Further, the courts have noted that "[t]he right not to have intimate facts concerning one's life disclosed without one's consent...is a venerable one whose constitutional significance we have recognized...."[8]

The right to privacy of personal information, including health information, is recognized under the tort law or statutory law of all 50 states, and 10 states (Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington) include a specific right to privacy in their state constitutions.

In addition, the right to not have one's health information disclosed without one's consent is a core concept of both the Hippocratic Oath and the ethical standards of "virtually all health professions,"[9] The American Medical Association (AMA) recently re-affirmed this ethical policy in the context of electronic health information systems:

> "Our AMA policy is that where possible, informed consent should be obtained before personally identifiable health information is used for any purpose."[10]

The ethical principles of other professional associations similarly provide:

> "Confidentiality of the patient's communications is a basic patient's right and an essential condition for effective psychoanalytic treatment and research. A psychoanalyst must take all measures necessary to not reveal present or former patient confidences without permission, nor discuss the particularities observed or inferred about patients outside consultative, educational or scientific contexts."[11]

Finally, the U.S. Supreme Court has found, based on the "reason and experience" of the country, that communications between a patient and a

---

[7] Gruenke v. Seip, 225 F.3d 290, 302-03 (3rd Cir. 2000); Sterling v. Borough of Minersville, 232 F.3d 190, 198 (3rd Cir. 2000).

[8] Sterling v. Borough of Minersville, 232 F.3d at 195.

[9] Finding of the National Committee on Vital and Health Statistics, report to HHS, p. 3 (June 22, 2006).

[10] American Medical Association, Report 19 of the Board of Trustees (A-07), Patient Information in the Electronic Medical Record.

[11] The American Psychoanalytic Association, Principles and Standards of Ethics for Psychoanalysts, Guiding General Principles, IV. Confidentiality.

psychotherapist, are subject to a "psychotherapist-patient privilege" which can only be waived by the patient.[12] The psychotherapist-patient privilege recognized at the federal level has also been recognized by all 50 states and the District of Columbia. The Supreme Court has noted that this privilege serves both the interest of the individual and the public in permitting access to effective psychotherapy and that unless such a privilege were recognized, communications essential for effective psychotherapy would simply not occur. At least 43 states recognize a physician-patient privilege under state law.

The Health Information Technology for Economic and Clinical Health (HITECH) Act recognized and preserved privileges under federal statutory law.[13] The HITECH Act also expressly preserved all existing state laws that afford "more stringent" privacy protections.[14]

So, the right to privacy and security for health information is well established and yet the right to privacy is not one of the rights listed in the HIPAA "Privacy" Rule (45 C.F.R. § 164.520(b)(1)(iv)), and the term "privacy" is the only key term that is not defined in Subtitle D of Title XXX of the HITECH Act entitled "Privacy." The right to privacy traditionally has been defined as the right of the individual to have some *control* over the disclosure of personal health information.[15] The National Committee on Vital and Health Statistics found, based on extensive research, that health information privacy is generally accepted as meaning, "an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data."[16]

As the National Committee on Vital and Health Statistics found after 18 months of hearings on the issue, "[a]ny system of personal health information collection, storage, retrieval, use and dissemination requires the utmost trust of the public."[17] Individuals cannot trust an electronic health information system unless they can be assured that, in such a system, their right to privacy for health information will be both recognized and protected.

---

[12] Jaffee v. Redmond, 116 S. Ct. 1923 (1996).
[13] HITECH Act, section 13421(c).
[14] HITECH Act, section 13421(a).
[15] HHS finding, 65 Fed. Reg. at 82,465; United States v. Westinghouse, 638 F.2d 570, 577, n. 5.
[16] NCVHS letter to Secretary Leavitt, p. 1 (June 22, 2006).
[17] NCVHS letter to Secretary Leavitt, p. 3.

Tab 2

BASIC PRIVACY PRINCIPLES FOR QUALITY HEALTH CARE

Federal law should include at least the following basic principles to preserve the individuals' right to health information privacy.

1. **Recognition of the right to privacy--Privacy provisions in federal law should recognize that individuals have a right to health information privacy.[1]**

2. **Ability to exercise right to privacy--Individuals should be permitted to exercise their right to health information privacy by choosing whether to give their written or electronic informed consent for disclosures and redisclosures of their identifiable health information, unless otherwise required by law.[2]**

3. **Right to privacy for specific information--Individuals should be allowed to limit the disclosure of certain especially sensitive health information (such as mental health, genetic, HIV/AIDS, and drug and alcohol treatment information) to only designated practitioners or for specific purposes.[3]**

4. **Right attaches to information--The privacy protections should apply to any individual or entity that handles personal health information.[4]**

---

[1] This "reasonable expectation" of privacy for health information has been recognized repeatedly by courts at every level of the federal judiciary. Ferguson v. City of Charleston, 532 U.S. 67 (2001); Whalen v. Roe, 429 U.S. 589 (1977); U.S. v. Scott, 424 F.3d 888 (9th Cir. 2005); Douglas v. Dobbs, 419 F.3d 1097 (10th Cir. 2005); Tucson Woman's Clinic v. Eden, 371 F.3d 1173 (9th Cir. 2004).

[2] This ability to have some control over the disclosure of one's health information has been identified as the essence of the right to health information privacy. HHS Finding, 65 Fed. Reg. at 82,465; U.S. v. Westinghouse, 638 F.2d 570, 577, n. 5 (3rd Cir. 1980). The ability to have some control over disclosures is also the core concept of the right to health privacy "now contained in the codes of ethics of virtually all health professionals." Finding of National Committee on Vital and Health Statistics (NCVHS), letter to Secretary Leavitt, p. 3 (June 22, 2006). See e.g., AMA, Current Opinions of Council on Ethical and Judicial Affairs, E-5.05 (1998). HHS included consent as a requirement for routine disclosures in the Original HIPAA Health Information Privacy Rule (65 Fed. Reg. at 82,474). The Amended Rule, which dropped the requirement, made clear that nothing in that rule was intended to eliminate or supplant this ethics standard. (67 Fed. Reg. at 53,212).

[3] Most states provide special privacy protections for these types of information. The NCVHS has found that the individual's right to limit access to certain kinds of health information (such as psychiatric records) is recognized in Australia, Great Britain, Canada, and Denmark. Privacy and Confidentiality in the Nationwide Health Information Network, NCVHS letter to Secretary of HHS, p. 6 (June 22, 2006).

[4] The NCVHS has noted that the HIPAA Privacy Rule is inadequate for a national electronic health information system because it only applies to "covered entities involved in claims processing." NCHVS letter to Secretary of HHS, p. 9 (June 22, 2006). More recently, NCVHS recommended that:

> HHS and the Congress should move expeditiously to establish laws and regulations that will ensure that all entities that create, compile, store, transmit, or use personally identifiable health information are covered by a federal privacy law. This is necessary to assure the public that the NHIN, and all of its components, are deserving of their trust.

5. **Meaningful relief for privacy violations--The privacy protections should provide individuals with a right to obtain damages and other relief where a reasonable person would have known that a disclosure was improper.[5]**

6. **Notification of privacy breaches--The privacy protections should require notification of actual or suspected privacy breaches to individuals whose privacy has been compromised.[6]**

7. **Preservation of state law and ethical standards--Nothing in the privacy protections should be construed as superseding, altering, or affecting (in whole or in part) any statute, regulation, order, or other interpretation in effect in any State or any standard of professional ethics that affords any person privacy and security protections greater than the privacy and security protections in federal law.[7]**

8. **Preservation of privileged communications--The privacy of health information protected by physician-patient or psychotherapist-patient privileges recognized under federal or state law should not be supplanted or limited by federal legislation. Any disclosure of health information authorized by a patient for the purposes of obtaining health insurance payment or coverage should not result in a waiver of any privilege.[8]**

9. **Definitions--The terms health information privacy, confidentiality and security should have the following meanings:**

   Health information privacy should mean an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data.

NCVHS letter to Secretary Leavitt, p. 3 (June 21, 2007). Also, the Joint Position Statement on Health Information Confidentiality by the American Medical Informatics Association and the American Health Information Management Association provides that "health information privacy protections must follow [health information] no matter where it resides." (July 2006).

[5] HHS has determined that all 50 states recognize in tort law a common law or statutory right to privacy. 65 Fed. Reg. at 82,464.

[6] Such breach disclosure laws have been adopted in at least 36 states. The Joint Position Statement of AMIA and AHIMA also supports this principle.

[7] As noted, HHS has taken the position that more stringent state health privacy protections and standards of professional practice should not be supplanted by electronic information standards. 67 Fed. Reg. at 53,212.

[8] A psychotherapist-patient privilege is recognized under federal law and the laws of all 50 states and the District of Columbia. Jaffee v. Redmond, 518 U.S. 1 (1996). A physician-patient privilege is recognized in 43 states and the District of Columbia. "The State of Health Privacy," Health Privacy Project (2000).

Confidentiality should mean the obligations of those who receive information to respect the privacy interests of those to whom the data relate.

Security means the physical, technological or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure.[9]

Adopted by the American Psychoanalytic Association

For more information, contact:

Jim Pyles
Powers, Pyles, Sutter & Verville, P.C.
1501 M Street, N.W.
Washington, D.C. 20005
(202) 466-6550
jim.pyles@ppsv.com

[9] These definitions have been adopted by the Institute of Medicine and have been recommended by the National Committee on Vital and Health Statistics, report to the Secretary of HHS, p. 2 (June 22, 2006).

Tab 3

Chronology of Electronic Health Breaches

The following information has been obtained from the "Chronology of Data Breaches" portion of the Privacy Rights Clearinghouse website. This chart is only a compilation of electronic health breaches reported in the press.

Location:	Date Made Public:	Name:	Type of Breach:	Number of Records:
Alabama	6/20/2006	University of Alabama	In February a computer was stolen from a locked office of the kidney transplant program at the University of Alabama at Birmingham that contained confidential information of donors, organ recipients and potential recipients including names, Social Security numbers and medical information.	9,800
Alabama	2/2/2007	U.S. Dept. of Veteran's Affairs, VA Medical Center	An employee reported a portable hard drive stolen or missing that might contain personal information about veterans including Social Security numbers.	583,000
Alabama	4/5/2007	DCH Health Systems	An encrypted disc and hardcopy documents containing retirement benefit information including Social Security numbers and other personal information were lost. Tracking data indicates the package was delivered to the addressee's building, but the intended recipient never received the package.	6,000
Alabama	8/11/2007	Providence Alaska Medical Center	A laptop computer that contains the personal information of patients is missing. On the laptop there maybe names, medical record numbers, dates of birth, patient diagnoses, Social Security numbers and addresses.	250
Alabama	11/5/2007	Alabama Department of Public Health	The personal information, including the names, ages and Social Security numbers of families enrolled in the state's ALL Kids health care coverage program, were accidentally sent to the wrong families last week. 1,554 affected families were alerted that some of their confidential information might have been released.	1,554
Arkansas	7/2/2008	Baptist Health	Due to a breach by an unauthorized person in the information systems, there is a possibility that some personal information, such as name, address, date of birth, Social Security number, and reason for coming to Baptist Health. No information in the patient's "medical records" and no information about the patient's diagnosis or prognosis was accessed.	1,800
Arkansas	7/20/2009	St. Vincent Health System	A physician and two former employees of the St. Vincent Health System pleaded guilty today to misdemeanor federal charges for accessing the medical records of slain television anchor Anne Pressly. All three said they accessed Pressly's files out of curiosity.	1
California	3/11/2005	Kaiser Permanente	A disgruntled employee posted informaton on her blog noting that Kaiser Permanente included private patient information on systems diagrams posted on the Web. UPDATE (6/21/2005):	140
California	4/8/2005	San Jose Med. Group	Stolen computer	187,000
California	4/15/2005	CA Dept. of Health Services	Stolen laptop	21,600
California	9/19/2005	Children's Health Council	Stolen backup tape	5,000-6,000
California	7/27/2006	Kaiser Permanente Northern Calif. Office	A laptop was stolen containing names, phone numbers, and the Kaiser number for each HMO member. The data file did not include SSNs. The data was being used to market Hearing Aid Services to Health Plan members.	160,000
California	8/18/2006	Calif. Dept. of Mental Health	Computer tape with employees' names, addresses, and SSNs has been reported missing. Employees were notified Aug. 17 by e-mail.	9,468

California	9/15/2006	Mercy Medical Center	A memory stick containing patient information was found July 18 by a local citizen on the ground at the County Fairgrounds near the hospital's information booth. It was returned to the hospital 4 weeks later. Data included names, SSNs, birthdates, and medical records.	295
California	2/14/2007	Kaiser Medical Center	A doctor's laptop was stolen from the Medical Center containing medical information of 22,000 patients. But only 500 records contained SSNs.	22,000
California	4/18/2007	University of CA, San Francisco	A computer file server containing names, contact information, and Social Security numbers for study subjects and potential study subjects related to studies on causes and cures for different types of cancer was stolen from a locked UCSF office. For some individuals, the files also included personal health information.	3,000
California	7/28/2007	Yuba County Health and Human Services	A laptop stolen from building contained personally identifiable information of individuals whose cases were opened before May 2001. The laptop was being used as a backup system for the county's computer system. The data include Social Security numbers, birth dates, driver's license numbers and other private information.	70,000
California	9/9/2007	McKesson	McKesson Health-care services company, is alerting thousands of its patients that their personal information is at risk after two of its computers were stolen from an office.	Unknown
California	12/10/2007	Sutter Lakeside Hospital	A laptop computer containing personal and medical information of approximately 45,000 former patients, employees and physicians has been stolen from the residence of a contractor.	45,000
California	2/27/2008	Health Net Federal Services	Thousands of doctors in eleven states had their personal information openly posted on a company website. Social Security numbers were part of the personal information exposed. The states involved include Wisconsin, Michigan, Illinois, Indiana, Ohio, Pennsylvania, Tennessee, Iowa, Missouri, Kentucky and West Virginia.	103,000
California	3/19/2008	UCLA Medical Center	UCLA Medical Center has moved to fire 13 employees and suspended six others for unauthorized access to confidential medical records.	900
California	3/26/2008	Presbyterian Intercommunity Hospital	About 5,000 past and current employees at Presbyterian Intercommunity Hospital had their private information stolen. The data included Social Security numbers, birth dates, full names and other records stored on a desktop computer that was stolen.	5,000
California	5/6/2008	Finjan	Researchers at security vendor Finjan uncovered a server containing the sensitive email and Web-based data of thousands of people, including healthcare information, credit card numbers and business personnel documents and other sensitive data. Finjan notified more than 40 major international financial institutions located in the United States, Europe and India whose customers were compromised as well as various law enforcements around the world. Server logs contained a mountain of healthcare information, including personal data, health data, treatment, medications, insurance details, Social Security Numbers, and healthcare providers' data, including physician's name. Banking data, including credit card numbers and account login numbers were also discovered on the server.	5,878
California	12/23/2008	Cedars-Sinai Medical Center	A former billing department employee is in custody on $895,000 bail for allegedly stealing the personal information of 1,000 hospital patients and using it to bilk insurance companies.	1,000

California	2/6/2009	Kaiser Permanente	A law enforcement agency seized a computer file with Kaiser data from a person who was subsequently arrested. The suspect was not a Kaiser employee. Kaiser Permanente is notifying nearly 30,000 Northern California employees that the security breach may have led to the release of their personal information. The stolen information included names, addresses, dates of birth and Social Security numbers for Kaiser employees.	30,000
California	4/1/2009	Palo Alto Medical Foundation	A laptop computer recently stolen at the Palo Alto Medical Foundation's Santa Cruz office contained personal and medical information of 1,000 Santa Cruz County patients.	1,000
California	4/22/2009	Marian Medical Center	Recent patients of the emergency room and Urgent Care Center have been alerted that a Blackberry containing patient information was stolen from the hospital. The Blackberry contained an email message that included patient information, such as Social Security numbers, dates of birth and medical histories.	3,200
California	5/15/2009	Kaiser Permanente Bellflower Medical Center	The California hospital where Nadya Suleman's octuplets were born has been fined $250,000 for failing to stop employees from snooping into medical files on the famous case. Hospital officials discovered that 23 unauthorized workers examined Suleman's medical records.	1
California	6/30/2009	Sutter Health	Hundreds of current and former employees with Sutter Health had their personal data compromised. The company's Sacramento Sierra region were contacted by a computer repair shop. "The repair people did the right thing and told us they had our laptop," said Sutter Communication Coordinator . The laptop contained names and Social Security numbers of 6,000 Sutter Health workers.	6,000
California	7/16/2009	Moores Cancer Center	A hacker breached the center's computers and gained access to patients' personal information.	30,000
California	9/22/2009	Sagebrush Medical Plaza/Kern Medical Center	Thousands of patients at a Kern County health clinic have been warned their personal information could have been stolen. A break-in happened at the Sagebrush Medical Plaza in July, and Kern Medical Center officials have notified 31,000 patients to take precautions against possible identity theft. One or more unknown individuals broke into a locked storage area that contained confidential patient information. All patient information has now been moved to a location inside the clinic building.	31,000
California	1/12/2010	Valley Kaiser	An electronic storage device stolen from an employee's car in Sacramento last month contained health information from 15,500 patients, including about 800 in the Fresno area. Information included patient names, medical-record numbers and, for some individuals, ages, dates of birth, gender, phone numbers and other information related to their care and treatment.	15,500
California	2/9/2010	California Department of Health Care Services	The personal security of nearly 50,000 people may have been breached by the California Department of Health Care Services. Social Security numbers were printed on the address labels of letters that were mailed by the department. State employees mistakenly included the numbers in a list of patient addresses. The list was sent to an outside contractor, who printed and mailed the envelopes.	50,000

California / Connecticut	1/4/2008	Health Net	Thousands of Health Net employees in Connecticut and other states have been notified that their names and Social Security numbers were on a laptop computer that was stolen more than a month ago from a company vendor. The laptop had information on about 5,000 employees companywide and an undisclosed number of health-care providers outside the Northeast.	5,000
Colorado	5/4/2005	CO. Health Dept.	Stolen laptop	1,600
Colorado	11/28/2006	Kaiser Permanente Colorado -- its Skyline and Southwest offices	A laptop was stolen from the personal car of a Kaiser employee in California on Oct. 4. It contained names, Kaiser ID number, date of birth, gender, and physician information. The data did not include SSNs.	38,000
Colorado	5/24/2007	Beacon Medical Services	Private medical and financial information including patient records from at least 10 Colorado clinics and hospitals, and one hospital in Peoria, Illinois that should have been only accessible through VPN access were inadvertently available on the Internet.	5,000
Colorado	12/7/2007	Beacon Medical Services	Detailed, personally identifiable medical records of thousands of Colorado residents were viewable on a publicly accessible Internet site for an uncertain period of time. The data included details of patients' visits to emergency rooms -- what ailments they complained of, diagnoses, treatments, and medical histories, along with the patients' names, occupations, addresses, phone numbers, insurance providers, and in some cases, Social Security numbers. The company is trying to determine the exact number of patients affected, but Beck says the number looks to be fewer than 5,000.	Unknown
Colorado	9/28/2009	Penrose Hospital	Officials at Penrose Hospital believe someone has stolen the personal information of 175 patients. The missing information consists of names, addresses, phone numbers, Social Security numbers and the reason for the patients' visits. The information was stored on a computer print-out and kept in a binder stored in a cabinet. The print out has gone missing.	175
Connecticut	4/26/2006	Aetna -- health insurance records for employees of 2 members, including Omni Hotels and the Dept. of Defense NAF	Laptop containing personal information including names, addresses and Social Security numbers of Dept. of Defense (35,253) and Omni Hotel employees (3,000) was stolen from an Aetna employee's car.	38,000
Connecticut	5/28/2009	Aetna	Aetna has contacted 65,000 current and former employees whose Social Security numbers may have been compromised in a Web site data breach. The breach was a spam campaign showing that the intruders successfully harvested e-mail addresses from the Web site, although it's not clear if SSNs were also obtained. The spam purported to be a response to a job inquiry and requested more personal information. Aetna sent letters last week notifying the 65,000 people whose SSNs were on the site of the breach.	65,000
Connecticut	11/18/2009	Health Net	The personal information for almost half a million Connecticut residents could be at risk after a portable disk drive disappeared from Health Net six months ago. Health Net is a regional health plan and the drive included health information, Social Security number and bank account numbers for all 446,000 Connecticut patients, 1.5 million nationally. The information had been compressed, but not encrypted, although a specialized computer program is required to read it. Patients in Arizona, New Jersey and New York were also affected.	1,500,000

Florida	2/16/2006	Blue Cross and Blue Shield	Contractor sent names and Social Security numbers of current and former employees, vendors and contractors to his home computer in violation of company policies.A judge today ordered a former computer consultant to reimburse the Jacksonville-based health insurer $580,000 for expenses related to his theft .	27,000
Florida	6/16/2006	ING	Two ING laptops that carried sensitive data affecting of Jackson Health System hospital workers were stolen in December 2005. The computers, belonging to financial services provider ING, contained information gathered during a voluntary life insurance enrollment drive in December and included names, birth dates and Social Security numbers.	8,500
Florida	9/9/2006	Cleveland Clinic	A clinic employee stole personal information from electronic files and sold it to her cousin, owner of Advanced Medical Claims, who used it to file fraudulent Medicare claims totaling more than $2.8 million. Information included names, SSNs, birthdates, addresses and other details. Both individuals were indicted.	1,100
Florida	7/7/2008	Florida Agency for Health Care Administration	A security breach in the Organ and Tissue Donor Registry may have exposed thousands of donors' personal information, including their Social Security numbers. Other data included donors' names, addresses, birth dates and driver license numbers.	55,000
Florida	7/17/2008	Bristol-Myers Squibb	A backup computer-data tape containing employees' personal information, including Social Security numbers, was stolen recently. The backup data tape was stolen while being transported from a storage facility. The information on the tapes included names, addresses, dates of birth, Social Security numbers and marital status, and in some cases bank-account information. Data for some employees' family members also were on the tape.	42,000
Florida	8/14/2008	Wuesthoff Medical Center	Hundreds of people in Brevard County found out their personal information was stolen. Names, Social Security numbers and even personal medical information were posted on the Internet.	500
Florida	7/31/2009	Jackson Memorial Hospital	A Miami man was charged with buying confidential patient records from a Jackson Memorial Hospital employee over the past two years, and selling them to a lawyer suspected of soliciting the patients to file personal-injury claims.	Unknown
Florida	9/2/2009	Naval Hospital Pensacola	Naval Hospital Pensacola will be notifying thousands of beneficiaries who use its pharmacy services, following the disappearance of a laptop computer. The computer's database contains a registry of 38,000 pharmacy service customers' names, Social Security numbers and dates of birth on all patients that used the pharmacy in the last year. It does not contain any personal health information.	38,000
Florida	10/15/2009	Halifax Health	A laptop computer from a Halifax Health employee's vehicle in Orange County was stolen -- which might have contained password protected patient information.	33,000

Florida	2/8/2010	AvMed Health Plans	AvMed Health Plans announced that personal information of some current and former subscribers may have been compromised by the theft of two company laptops from its corporate offices in Gainesville. The information included names, addresses, phone numbers, Social Security numbers and protected health information. The theft was immediately reported to local authorities but attempts to locate the laptops have been unsuccessful. AvMed determined that the data on one of the laptops may not have been protected properly, and approximately 80,000 of AvMed's current subscribers and their dependents may be affected. An additional approximate 128,000 former subscribers and their dependents, dating back to April 2003, may also have been affected.	208,000
Georgia	8/4/2006	PSA HealthCare	A company laptop was stolen from an employee's vehicle in a public parking lot July 15. It contained names, addresses, SSNs, and medical diagnostic and treatment information used in reimbursement claims.	51,000
Georgia	4/10/2007	Georgia Dept. of Community Health	A computer disk containing personal information including addresses, birthdates, dates of eligibility, full names, Medicaid or children's health care recipient identification numbers, and Social Security numbers went missing from a private vendor, Affiliated Computer Services (ACS), contracted to handle health care claims for the state.	2,900,000
Georgia	10/2/2007	Athens Regional Health Services	A computer missing from a Regional First Care clinic in Watkinsville held the personal information of more than 1,400 people, according to Athens Regional Health Services. Workers first noticed on Sept. 24 that the computer was missing. The computer held Social Security numbers for 85 people, some health information for 545 people and the name, address and/or telephone numbers of 811 people. No credit card or other financial information was stored on the computer, which was a backup server for the Watkinsville clinic.	1,400
Georgia	4/8/2008	WellCare Health Plans Inc.	Private records of members of health insurance programs for the poor or working poor were accidentally made available on the Internet for several days. Those whose data was made available on the Internet included members of Medicaid, the federal health program for the poor, and PeachCare for Kids, a federal-state insurance plan for children of the working poor. About 10,500 members' Social Security numbers may have been viewed by unauthorized people on the Internet, all members of Medicaid or PeachCare. There is a possibility that an initial 59,000 members may have had some personal information made accessible.	71,000
Georgia	7/25/2008	Grady Memorial Hospital	Hospital records were stolen. It remains unknown how many patient records were stolen, which patients were affected or how the records were stolen. The records pertained to recorded physician comments that Grady sent to a vendor to transcribe into medical notes. The records were stolen from a subcontractor employed by the vendor.	Unknown
Hawaii	10/21/2005	Wilcox Memorial Hospital	Lost backup tape	130,000
Hawaii	1/25/2007	Washiawa Women, Infants and Children program (WIC)	A WIC employee apparently stole the personal information of agency clients, including SSNs, and committed identity theft on at least 3 families and perhaps 2 more. The Health Director said the agency will no longer use SSNs in its data base.	11,500

Hawaii	7/22/2009	A Honolulu hospital	In June 2009, a Hawaii woman was sentenced to a year in prison for illegally accessing another woman's medical records and posting on MySpace that she had HIV. The State of Hawaii brought charges under a state law that criminalizes unauthorized access to a compute as a class B felony. The defendant was employed by a hospital and had access to patient medical records.	Unknown
Illinois	2/18/2005	Univ. of Chicago Hospital	Dishonest insider	85
Illinois	3/18/2009	Walgreens Health Initiative/KRS	Names, dates of birth and Social Security numbers of roughly 28,000 state retirees were e-mailed to the Kentucky Retirement Systems without being properly encrypted for security purposes by its pharmacy benefit provide. The e-mail contained dates of birth, Social Security numbers and health insurance claim numbers but not personal health information. The file contained information only on members who were both Medicare-eligible and used the retiree pharmacy benefit through Walgreens in 2007.	28,000
Illinois	10/6/2009	BlueCross BlueShield Assn.	A file containing identifying information for every physician in the country contracted with a Blues-affiliated insurance plan was on a laptop computer stolen from a BlueCross BlueShield Assn. employee. The file included the name, address, tax identification number and national provider identifier number for about 850,000 doctors. Some 16% to 22% of those physicians listed -- as many as 187,000 -- used their Social Security numbers as a tax ID or NPI number.	187,000
Indiana	10/23/2006	Sisters of St. Francis Health Services via Advanced Receivables Strategy (ARS), a Perot Systems Company	On July 28, 2006, a contractor working for Advanced Receivables Strategy, a medical billing records company, misplaced CDs containing the names and SSNs of 266,200 patients, employees, physicians, and boad members of St. Francis hospitals in Indiana and Illinois. Also affected were records of Greater Lafayette Health Services. The disks were inadvertently left in a laptop case that was returned to a store. The purchaser returned the disks. The records were not encrypted even though St. Francis and ARS policies require encryption.	266,200
Indiana	1/2/2007	Deaconess Hospital	A computer missing from the hospital holds personal information, including SSNs, of 128 respiratory therapy patients.	128
Indiana	3/14/2007	Wellpoint's Empire Blue Cross and Blue Shield unit in NY	An unencrypted disc containing patient's names, Social Security numbers, health plan identification numbers and description of medical services back to 2003 was lost en route to a subcontractor.	75,000
Indiana	3/20/2007	Health Resources, Inc.	From Jan 24, 2007 to Feb 6, 2007, a Web site glitch allowed employers with access to private health information to obtain the name, address, Social Security number, dependent names and birthdates of other patients.	2,031
Indiana	7/24/2007	St. Vincent Hospital	A security lapse compromised names, addresses and Social Security numbers.	51,000
Indiana	11/15/2007	Roudebush Veteran's Administration Medical Center	Two personal computers and a laptop computer were allegedly stolen from an unsecured room. One of the stolen computers contained the names, Social Security numbers and dates of service of approximately 12,000 veterans.	12,000
Indiana	2/7/2008	Memorial Hospital	A laptop containing the personal information of full and part time employees and retirees is missing. The missing computer contains their names, addresses, birth dates, ID numbers and Social Security numbers.	4,300

Indiana	4/8/2008	WellPoint	Personal information that may have included Social Security numbers and pharmacy or medical data for customers in several states was exposed online over the past year.	128,000
Indiana	1/12/2010	AIG Medical Excess	A 28-year-old Indianapolis man was sentenced today to two years in state prison for trying to extort $208,00 from an insurance company after stealing a computer server. In March 2006, the man burglarized the Indianapolis office of AIG Medical Excess, threatening to release clients' personal data on the Internet. The server contained the names of more than 900,000 insured persons, as well as their personal identifying information, and confidential medical information and e-mail communications. At the time of the burglary, the man was an employee of a private security firm that provided security services to the insurance company. On July 23, 2008, Stewart delivered a package to the insurance company. The package included a letter stating that he possessed the stolen server and its confidential data. He asked for $1,000 a week for four years, but the FBI and others intervened. The Indiana State Police, the Indiana Department of Natural Resources, Indianapolis Metropolitan Police Department, and Attorney General also were part of the investigation.	900,000
Kansas	7/9/2008	Wichita Radiological Group	A former employee stole patient records before being fired from the Wichita Radiological Group. Tens of thousands of patient records were in the database could have been compromised.	Unknown
Kentucky	6/2/2006	Humana	Personal information of Humana customers enrolled in the company's Medicare prescription drug plans could have been compromised when an insurance company employee called up the data through a hotel computer and then failed to delete the file.	17,000
Kentucky	11/16/2006	American Cancer Society	An unspecified number of laptop computers were stolen from the Louisville offices of the American Cancer Society. It is not clear what personal information was exposed, if any.	Unknown
Kentucky	10/27/2009	Baptist Hospital East	Hundreds of people in Kentuckiana are worrying about identity theft after their employer accidentally released their social security numbers. 350 names of hospital employees appear on a list that was circulated in an e-mail and so did their Social Security numbers.	350
Louisiana	9/30/2008	Blue Cross & Blue Shield	A document containing the personal data was accidentally attached to a general e-mail being sent out to brokers notifying them of a software upgrade. Information such as Social Security numbers, phone numbers and addresses were exposed.	1,700
Maryland	2/7/2007	Johns Hopkins University and Johns Hopkins Hospital	Johns Hopkins reported the disappearance of 9 backup computer tapes containing personal information of employees and patients, Eight of the tapes contained payroll information on 52,000 past and present employees, including SSNs and in some cases bank account numbers. The 9th tape contained "less sensitive" information about 83,000 hospital patients.	135,000
Maryland	2/8/2007	St. Mary's Hospital	A laptop was stolen in December that contained names, SSNs, and birthdates for many of the Hospital's patients.	130,000
Maryland	4/24/2007	Baltimore County Dept. of Health	A laptop containing personal information including names, date of birth, Social Security numbers, telephone numbers and emergency contact information of patients who were seen at the clinic between Jan. 1, 2004 and April 12 was stolen.	6,000

Maryland	9/1/2007	Johns Hopkins Hospital	A desktop computer containing the personal information of 5,783 Johns Hopkins Hospital patients was stolen. The computer included patients' names, Social Security numbers, birth dates and medical histories.	5,783
Maryland	3/24/2008	National Institutes of Health	A laptop was stolen from the trunk of a car. It contained information about heart disease patients, including their names, dates of birth and diagnoses of their medical conditions.	4,359
Maryland	4/11/2009	Peninsula Orthopaedic Associates	As many as 100,000 patients of Peninsula Orthopaedic Associates are being warned to protect themselves against identity theft after tapes containing patient information were stolen. Patients also were advised to keep an eye on benefits statements from their health insurance companies since they may also be at risk for medical identity theft. The records from Peninsula Orthopaedic were stolen March 25 while in transport to an off-site storage facility. Patients' personal information including their Social Security numbers, employers and health insurance plan numbers may have been among the information stolen.	100,000
Maryland	5/12/2009	Johns Hopkins	An investigation suggests a former employee who worked in patient registration may have been linked to a scheme to create fake drivers' licenses in Virginia. The employee had access to information such as name, address, telephone number, mother and fathers names, dates of birth and Social Security numbers, but not to any health or medical information.	10,000
Maryland	11/20/2009	Johns Hopkins Medicine	A woman who worked as a patient services coordinator for Johns Hopkins Medicine has been sentenced to 18 months in prison for stealing patient information. Thirty-one-year-old woman of Baltimore was also ordered to pay more than $200,000 in restitution. According to her plea agreement and court documents, from August 2005 to April 2007, the woman provided a conspirator with names, Social Security numbers and other identifying information of more than 100 current and former patients of Johns Hopkins. That information was used to apply for credit.	100
Massachusetts	11/30/2007	Prescription Advantage	The state of Massachusetts is warning 150,000 members of its Prescription Advantage insurance program that their personal information may have been snatched by an identity thief. Local authorities arrested a lone identity thief who had been using information taken from the program in an attempted identity theft scheme. Although the thief used information from just a small number of participants in the scheme, state data-breach laws require that the 150,000 people who could have possibly been affected by the breach be contacted.	150,000
Massachusetts	1/24/2008	Fallon Community Health Plan	A vendor computer containing personal information on patients of Fallon Community Health Plan has been stolen. The data included names, dates of birth, some diagnostic information and medical ID numbers. Some of which may be based on Social Security numbers.	30,000
Massachusetts	4/22/2008	Central New England HealthAlliance	Personal data could be at risk of exposure after a home health nurse reported that her handheld computer was missing. The unencrypted data include names, Social Security numbers, and health insurance records.	384
Massachusetts	4/22/2008	University of Massachusetts	Hackers breached the computer system used by UMass Amherst's Health Services, potentially gaining access to thousands of medical records. More than half of the student population at UMass Amherst are patients on record at the University Health Services.	Unknown

Massachusetts	2/3/2009	Baystate Medical Center	Several laptops were stolen from Baystate Medical Center's Pediatrics department. Some of those computers had patient information on them. All of the information is password protected and the computers had no financial or Social Security information on them.	Unknown
Michigan	8/22/2006	Beaumont Hospital	A vehicle of a home health care nurse was stolen from outside a senior center Aug. 5. Although it was recovered nearby, a laptop left in the rear of the car was not recovered. It contained names, addresses, SSNs, and insurance information of home health care patients.	28,400
Michigan	9/16/2006	Michigan Dept. of Community Health	Residents who participated in a scientific study were notified that a flash drive was discovered missing as of Aug. 4, and likely stolen, from an MDCH office.The portable memory device contained names, addresses, phone numbers, dates of birth, and SSNs of participants. The study tracked the long-term exposure to flame retardents ingested by residents in beef and milk.	4,000
Michigan	9/16/2006	Beaumont Hospital	The hospital mistakenly mailed medical reports on 3 patients to a retired dentist in Texas. Reports included name, test results, date of birth and patient ID numbers. The hospital admitted to both human and computer error. A new computer system mixed similar names, and staff did not catch it.	3
Michigan	8/15/2007	Greater Detroit Hospital	It's a repeat of a problem that emerged late last year at the Greater Detroit Hospital where metal thieves stripped everything from copper piping to windows, exposing rows of abandoned patient files. Neighbors said there are hundreds of boxes of patient files and payroll records inside, full of credit card and Social Security numbers.	Unknown
Michigan	9/19/2007	University of Michigan School of Nursing	Backup tapes containing patient information like Social Security numbers, patient names and addresses were stolen from the School of Nursing two weeks ago.	8,585
Michigan	12/15/2009	Detroit's Health Department	Police are investigating two incidents in which patients' medical records -- including social security numbers -- were stolen from the city's health department. The first theft occurred in late October when a flash drive was stolen from a health department employee's car. It contained files with birth certificate information for babies born in 2008 and the first half of 2009 whose parents reside in the 48202 and 48205 zip codes. Also a part of the files were information on the mothers' names and health conditions, the fathers' names, addresses, Medicaid numbers and social security numbers. The second incident happened over the Thanksgiving break when five computers were stolen from the immunization program at the department's Herman Kiefer Health Complex. One of the computers contained Medicare and Medicaid seasonal flu billing information for 2008.	5000
Minnesota	10/19/2006	Allina Hospitals and Clinics	A laptop stolen from a nurse's car on October 8 contains the names and SSNs of individuals in approximately 17,000 households participating in the Allina Hospitals and Clinics obstetric home-care program since June 2005.	17,000
Minnesota	12/5/2007	Memorial Blood Centers	A laptop computer holding donor information was stolen. About 268,000 donor records on this laptop computer contain a donor name in combination with the donor's Social Security number.	268,000

Minnesota	1/31/2008	University of Minnesota Reproductive Medicine Center	A doctor at the fertility clinic lost a flash drive that was used to back up his computer. The drive held details of infertility treatments for 3,100 patients going back to 1999. The lost drive included names, birthdates, and in some cases, diagnostic information, details of treatments, whether or not patients had conceived, baby names, and birth weights -- but apparently no SSNs or financial information.	3,100
Nevada	7/24/2008	Saint Mary's Regional Medical Center	A unauthorized person may have accessed the Saint Mary's database. The database, used for Saint Mary's health education classes and wellness programs, contained personal information such as names and addresses, limited health information and some Social Security numbers. The database did not contain medical records or credit card information.	128,000
Nevada	11/20/2009	University Medical Center	Someone at UMC is selling a compilation of the hospital's daily registration forms for accident patients. This is confidential information — including names, birth dates, Social Security numbers and injuries. Private information about accident victims	Unknown
Nevada	12/10/2009	University Medical Center	University Medical Center in Las Vegas is offering free use of a credit monitoring service to people whose confidential records may have been leaked to outsiders. Hospital officials were alerted last month that perhaps 141 accident victims' personal information was leaked Oct. 31 and Nov. 1. The information including Social Security numbers.	141
Nevada	1/25/2010	University Medical Center	For more than three months someone at University Medical Center illegally leaked the personal information of traffic accident victims — a breach of Social Security numbers, birth dates and more that only stopped when the Las Vegas Sun contacted the hospital about it.	Unknown
New Hampshire	6/9/2007	Concord Hospital	Names, addresses, dates of birth and Social Security numbers exposed on the internet "for a period of time,"security lapsed from a subcontractor that handles its online billing.	9,000
New Hampshire	3/19/2008	The Dental Network	A security breach of The Dental Network web site left access to member personal data, including names, Social Security numbers, addresses and dates of birth unprotected for approximately two weeks. The Dental Network is an independent licensee of the Blue Cross and Blue Shield Association.	75,000
New Hampshire	12/17/2008	New Hampshire Dept. of Health and Human Services	Health and Human Services mistakenly released the Social Security numbers and other personal information of Medicare Part D recipients. The information was mistakenly attached to a e-mail to health care organizations including nursing homes.	9,300
New Jersey	8/31/2006	Labcorp	During a break-in June 4 or 5, a computer was stolen that contained names and SSNs, but according to the company did not have birth dates or lab test results.	Unknown
New Jersey	1/29/2008	Horizon Blue Cross Blue Shield	More than 300,000 members names, Social Security numbers and other personal information were contained on a laptop computer that was stolen. The laptop was being taken home by an employee who regularly works with member data.	300,000
New York	2/17/2006	Mount St. Mary's Hospital	Two laptops containing date of birth, address and Social Security numbers of patients was stolen in an armed robbery in the New Jersey.	17,000

New York	6/14/2006	American Insurance Group(AIG), Indiana Office of Medical Excess, LLC	The computer server was stolen on March 31 containing personal information including names, Social Security numbers, birth dates, and some medical and disability information.	930,000
New York	7/17/2006	Vassar Brothers Medical Center	Laptop was stolen from the emergency department between June 23-26. It contained information on patients dating back to 2000, including SSNs and dates of birth.	257,800
New York	10/20/2006	Manhattan Veteran's Affairs Medical Center, New York Harbor Health Care System	On Sept. 6, an unencrypted laptop computer containing veterans' names, Social Security numbers, and medical diagnosis, was stolen from the hopsital.	1,600
New York	10/24/2006	Jacobs Neurological Institute	The laptop of a research doctor was stolen from her locked office at the Institute. It included records of patients and her research data.	Unknown
New York	5/11/2007	Highland Hospital	Two laptop computers, one containing patient information including Social Security numbers, were stolen from a business office. The computers were sold on eBay, and the one containing personal information was recovered.	13,000
New York	8/13/2007	Pfizer/Axia Ltd.	Axia Ltd. had notified Pfizer on June 14 of an incident in which two Pfizer laptops were stolen from a locked car. The laptops, which disappeared May 31 in Boston, included the names and Social Security numbers of health-care professionals who "were providing or considering providing contract services for Pfizer," according to the letter.	950
New York	11/21/2007	United Healthcare	United Healthcare posted the Social Security numbers of doctors at Columbia University's faculty practice on a public Web site. United posted the taxpayer identification numbers, some of which were Social Security numbers, alongside the names of 993 providers at Columbia who participate in the insurer's network. The list was supposed to be accessible to Columbia employees during the current open enrollment period	Unknown
New York	3/10/2008	Blue-Cross Blue-Shield of Western New York	A laptop hard-drive containing vital information about members has gone missing. Blue-Cross Blue-Shield of Western New York says it is notifying its members about identity theft concerns after one of it's company laptops went missing.	40,000
New York	4/7/2008	Pfizer Inc.	A laptop was stolen by a burglar from the home of a contractor who helps arrange planning travel and meetings for Pfizer. Information on the laptop included names, credit card numbers and, in some instances, credit card expiration dates, various addresses and phone numbers, hotel loyalty program numbers and other information. It did not appear that any Social Security numbers or PIN codes were exposed.	800
New York	4/11/2008	New York-Presbyterian Hospital/	An admissions employee is accused of selling 2,000 patients' data in an identity theft scheme and accessing nearly 50,000 records illegitimately. Records contained names, phone numbers and, in some cases, Social Security numbers of patients. The employee has since been charged with one count of conspiracy involving computer fraud, identity document fraud, transmission of stolen property and sale of stolen property.	50,000
New York	5/4/2008	Staten Island University Hospital	Computer equipment stolen from an administrator contained personal information from patients. Social Security numbers and health insurance numbers were contained in computer files on a desktop computer and the backup hard drive.	88,000

New York	5/12/2008	Pfizer	About 13,000 employees at Pfizer Inc., including about 5,000 from Connecticut, had their personal information compromised when a company laptop and flash drive were stolen. No Social Security numbers were on the laptop, but names, home addresses, home telephone numbers, employee ID numbers, positions and salaries were possibly compromised. Other information possibly lost included the department employees worked in, the Pfizer site where the employees worked, the name of employees' managers and descriptions of their jobs.	18,000
New York	2/6/2009	Catskill Regional Medical Center	A woman was fired for allegedly spying. The employee had access to company files. The files included Social Security numbers, birth dates, addresses and financial information.	431
North Carolina	6/21/2006	Cape Fear Valley Health System	Portable computer containing personal information of more than 24,000 people was stolen from ambulance of Cumberland Co. Emergency Medical Services on June 8th. It contained information on people treated by the EMS, including names, addresses and birthdates, plus SSNs of 84% of those listed.	24,350
North Carolina	11/7/2007	Carolinas Medical Center - NorthEast	A paramedic left a computer on the back bumper of an ambulance and then drove away. The laptop contains names, addresses, phone numbers and Social Security numbers of approximately 28,000 people who have been cared for by the Cabarrus County EMS over the last four years.	28,000
North Carolina	1/29/2008	Wake County (NC) Emergency Medical Services	A Panasonic Toughbook used by county paramedics to store patient information on ambulance runs went missing from the WakeMed emergency department and now is thought to have been stolen. The laptop contained names, addresses and Social Security numbers.	4,642
North Carolina	7/16/2008	Greensboro Gynecology Associates	A backup tape of patient information was stolen from an employee who was taking the tape to an off-site storage facility for safekeeping. The stolen information included patients' names, addresses, Social Security numbers, employers, insurance companies, policy numbers and family members.	47,000
North Carolina	11/5/2008	North Carolina Dept. of Health and Human Services	A laptop computer belonging to a Division of Aging and Adult Services employee was stolen. The computer contained information about people receiving home and community services.	Unknown
North Carolina	2/19/2009	Northeast Orthopaedics	Records of more than 1,000 patient visits to Northeast Orthopaedics, a large Albany surgical practice, have been posted on the Internet. The records appeared on the Web site visvabpo.com, which seems to be a defunct company in India called Visva BPO. Those records include patient names, birth dates and Social Security numbers.	1,000
North Carolina	4/13/2009	Moses Cone Hospital	Moses Cone Hospital is offering free credit monitoring to 14,380 patients after a laptop computer containing confidential information was stolen from a VHA employee's car. The information on the laptop, including patients' Social Security numbers.	14,380
North Carolina	10/13/2009	Pitt County Memorial Hospital	Patient names and Social Security numbers were placed onto a portable computer storage device, used to move the information between different computer systems. Employees have since discovered that USB flashdrive is missing from where it was stored.	1,700

North Carolina	12/4/2009	MedSolutions	For a period of time that has not been clearly defined the name, address, email, and taxpayer ID number (which in some cases is the physician's Social Security number) for an undetermined number of NC physicians could be viewed on the MedSolutions website. Access to this information apparently was not limited to physicians or physician staff. Based on the information available at the time of this posting, any person with an email address could enter physician names and view the information.	Unknown
Ohio	6/30/2005	Ohio State Univ. Med. Ctr.	Stolen laptop	15,000
Ohio	10/12/2005	Ohio State Univ. Medical Center	Exposed online. Appointment information including SSN, DOB, address, phone no., medical no., appointment reason, physician.	2,800
Ohio	3/1/2006	Medco Health Solutions	Stolen laptop containing Social Security numbers for State of Ohio employees and their dependents, as well as their birth dates and, in some cases, prescription drug histories.	4,600
Ohio	5/23/2006	Butler Co. Dept. of Mental Retardation & Developmental Disabilities	Three laptop computers were stolen "last month" from the agency's office. They contained personal information on mental health clients, including SSNs.	100
Ohio	6/2/2006	Buckeye Community Health Plan	Four laptop computers containing customer names, Social Security numbers, and addresses were stolen from the Medicaid insurance provider.	72,000
Ohio	10/26/2006	Akron Children's Hospital	Overseas hackers broke into two computers at Children's Hospital. One contains private patient data (including Social Security numbers) and the other holds billing and banking information.	235,903
Ohio	12/12/2006	Aetna / Nationwide / Wellpoint Group Health Plans via Concentra Preferred Systems	A lockbox holding personal information of health insurance customers was stolen Oct. 26. Thieves broke into an office building occupied by insurance company vendor, Concentra Preferred Systems. The lockbox contained computer backup tapes of medical claim data for Aetna and other Concentra health plan clients. Exposed data includes member names, hospital codes, and either SSNs or Aetna member ID numbers. SSNs of 750 medical professionals were also exposed. Officials downplay the risk by stating that the tapes cannot be used on a standard PC.	200,279
Ohio	1/25/2007	Ohio Board of Nursing	The agency's Web site posted names and SSNs of newly licensed nurses twice in the past 2 months. SSNs were supposed to have been removed before posting.	3,031
Ohio	12/1/2007	Community Blood Center/Battelle & Battelle LLC	Battelle & Battelle LLC was conducting an audit of the blood center's 401K plan when a laptop was stolen from a Battelle employee's vehicle. Up to 600 employees appeared to be affected.	600
Ohio	10/23/2008	Medical Mutual of Ohio	Eleven computer disks containing personal information on Ohio retirees and employees are missing, disks are most likely somewhere in the postal system. It seems insufficient postage was placed on the envelopes [containing the disks], therefore they are believed that they are likely to still be safe within the postal system.	36,000

Ohio	9/17/2009	Akron Children's Hospital	A 38-year-old Avon Lake, Ohio, man is set to plead guilty to federal charges after spyware he allegedly meant to install on the computer of a woman he'd had a relationship with ended up infecting computers at Akron Children's Hospital. He allegedly sent the spyware to the woman's Yahoo e-mail address, hoping that it would give him a way to monitor what she was doing on her PC. But instead, she opened the spyware on a computer in the hospital's pediatric cardiac surgery department, creating a regulatory nightmare for the hospital. Between March 19 and March 28 the spyware sent more than 1,000 screen captures via e-mail. They included details of medical procedures, diagnostic notes and other confidential information relating to 62 hospital patients. He was also able to obtain e-mail and financial records of four other hospital employees as well, the plea agreement states.	66
Ohio	1/21/2010	Columbus Public Health	An investigation is under way after hundreds of city health workers' personal information was stolen. Investigators have identified a person of interest in connection with the stolen information. The person of interest was an employee within the department over the past three years. Current employees and those who previously worked at the department within the last three years may be affected.	Unknown
Oklahoma	11/2/2006	McAlester Clinic and Veteran's Affairs Medical Center	Three disks containing billing information, patient names and Social Security numbers, were lost in the mail.	1,400
Oregon	1/25/2006	Providence Home Services	Stolen backup tapes, laptops and disks containing Social Security numbers, clinical and demographic information. In a small number of cases, patient financial data was stolen.	365,000
Oregon	8/15/2007	Sky Lakes Medical Center / Verus Inc.	The company that maintained the hospital's online bill payment system, transferred patient information from one server to another to perform maintenance but didn't take security measures, leaving information such as names, addresses and Social Security numbers exposed.	30,000
Oregon	3/6/2008	Cascade Healthcare Community	A computer virus may have exposed to outside eyes the names, credit card numbers, dates of birth and home addresses individuals who donated to Cascade Healthcare Community.	11,500
Oregon	11/1/2008	Veterans Affairs Medical Center	Personal information, including some Social Security numbers, of patients at the Veterans Affairs Medical Center in Portland was inadvertently posted on a public Web site.	1,600
Oregon	1/30/2009	Coos Bay Department of Human Services	A scammer made off with Social Security numbers after sending a virus online to a computer at the Department of Human Services office. A application that was installed recorded keystrokes and sent them to an external address. The information was taken from Coos County residents.	45
Oregon	12/28/2009	Providence Health	Providence Health Plans is re-issuing thousands of insurance cards after personal information was accidentally sent to the wrong policy-holders. Officials with Providence Health Plans say about 4,500 mailings were sent out with the incorrect group and member ID numbers, meaning that some policy holders received others' information. Officials noticed the problem Monday.	4,500
Pennsylvania	1/1/2006	University of Pittsburgh Medical Center, Squirrel Hill Family Medicine	6 Stolen computers. Names, Social Security numbers, birthdates	700

Pennsylvania	6/21/2006 (Date of letter sent to doctors. Date of news story is 7/28/2006)	Lancaster General Hospital	A desktop computer with personal information of hundreds of doctors was stolen from a locked office June 10. The unencrypted data included names, practice addresses and SSNS of physicians on medical and dental staff.	"Hundreds of local physicians"
Pennsylvania	1/5/2007	Dr. Baceski's office, internal medicine	A hard drive was stolen containing personal information on "hundreds of patients."	"hundreds of patients"
Pennsylvania	4/12/2007	Univ. of Pittsburgh, Med. Center	Personal information including names, Social Security numbers, and radiology images of patients were previously included in two medical symposium presentations that were posted on UPMC's Web site. Though the presentation was later removed in 2005, the presentations were apparently inadvertently re-posted on the site and only recently removed again.	88
Pennsylvania	9/11/2007	Pennsylvania Public Welfare Department	Two computers containing the mental health histories of more than 300,000 medical-assistance recipients were stolen. The computer work stations were taken during an overnight break-in at an office. The mental health information on the computers identified people by codes and not by name. The information also was protected by multiple passwords, but full names and Social Security numbers of nearly 2,000 people were also on the computers.	2,000
Pennsylvania	12/17/2007	West Penn Allegheny Health System	The names, Social Security numbers, phone numbers, addresses and patient care information of 42,000 patients were all on a laptop computer stolen from a nurse's home. Only home care and hospice patients could be impacted, not patients at the hospitals.	42,000
Pennsylvania	4/27/2008	General Internal Medicine of Lancaster	A laptop was stolen from a doctors office containing the Social Security numbers of patients.	Unknown
Pennsylvania	12/1/2009	Children's Hospital of Philadelphia	A laptop computer containing Social Security Numbers and other personal information was stolen from a car outside an employee's home on Oct. 20. The billing information on the computer was password-protected, but an analysis found it was "possible to decode the security controls on the laptop and gain access to the personal information."	943
Rhode Island	3/1/2007	Westerly Hospital	Patient names, Social Security numbers, contact information as well as insurance information were posted on a publicly-accessible Web site.	2,242
South Carolina	1/31/2008	South Carolina Department of Health and Environmental Control	A laptop containing the names and Social Security numbers of state health department employees is missing. The computer was inside a worker's vehicle when it was stolen last week from a convenience store. State officials say the password-protected computer contains personal information of state health department workers from Spartanburg, Cherokee, Union, Greenville and Pickens counties.	400
Tennessee	11/1/2005	Univ. of Tenn. Medical Center	Stolen laptop	3,800
Tennessee	8/17/2006	HCA, Inc.	10 computers containing Medicare and Medicaid billing information and records of employees and physicians from 1996-2006 were stolen from one of the company's regional offices. Some patient names and SSNs were exposed, but details are vague. Records for patients in hospitals in the following states were affected: CO, KS, LA, MS, OK, OR, TS, WA.	"thousands of files"
Tennessee	9/23/2006	Erlanger Health System	Records of hospital employees disappeared from a locked office on Sept. 15. They were stored on a USB "jump drive." Information was limited to names and SSNs. Those affected included anyone who went through job "status changes" from Nov. 2003 to Sept. 2006.	4,150

Tennessee	12/14/2006	Electronic Registry Systems affecting Emory University (Emory Hospital, Emory Crawford Long Hospital, Grady Memorial Hospital), Geisinger Health System (Pennyslvania), Williamson Medical Center	On Nov. 23, 2006, two computers (one desktop, one laptop) were stolen from Electronic Registry Systems, a business contractor in suburban Springdale, OH, that provides cancer patient registry data processing services. It contained the personal information (name, date of birth, Social Security number, address, medical record number, medical data and treatment information) of cancer patients from hospitals in Pennsylvania, Tennessee , Ohio and Georgia , dating back to 1977 at some hospitals.	63,000+
Tennessee	2/13/2008	Lifeblood	Laptop computers with birth dates and other personal information of roughly 321,000 blood donors are missing and presumed stolen. Stored inside both computers were names, birth dates and addresses at the time of the individual's last donation or attempted donation. In most cases, the donors' Social Security numbers were also stored, along with driver's licenses, telephone numbers, e-mail addresses, ethnicity, marital status, blood type and cholesterol levels. Social Security numbers had been used to track blood from the donor to the recipients.	321,000
Tennessee	5/22/2008	HealthSpring Inc.	A laptop computer containing personal information of about 450 state residents was stolen. The laptop, believed to contain names, dates of birth and Social Security numbers of about 9,000 individuals, was stolen from a HealthSpring employee's locked car.	9,000
Tennessee	4/12/2009	CBIZ Medical Management Professionals	The office of CBIZ Medical was broken into on Feb. 23. Among the items stolen was a computer belonging to the hospital with stored radiology reports related to some patients. Patients between December 2007 and Feb. 23, 2009, may have had records saved on the stolen computer.	Unknown
Tennessee	1/14/2010	BlueCross BlueShield	The theft of 57 hard drives from a BlueCross BlueShield of Tennessee training facility last October has put at risk the private information of approximately 500,000 customers in at least 32 states. The hard drives containing 1.3 million audio files and 300,000 video files. The files contained customers' personal data and protected health information that was encoded but not encrypted, including: Names and BlueCross ID numbers. In some recordings-but not all-diagnostic information, date of birth, and/or a Social Security number. BCBS of TN estimates that the Social Security numbers of approximately 220,000 customers may be at risk.	220,000
Tennessee	2/12/2010	BlueCross BlueShield	57 hard drives were stolen from a leased facility for BlueCross BlueShield. The drives contained data including protected health information of customers (which it calls 'members') of its health plan. The insurer sent out 220,133 notifications to tier 3 customers indicating that their personal information was included on the stolen drives. This information included name, address, BlueCross member ID number, diagnosis, Social Security number, and date of birth. A total of 301,628 current and former subscribers - customers whose plans extend to other individuals - will now be notified in the tier 2 category. 131,909 subscriber ID numbers were identified during the review of the customer service calls, and there were 168,719 family members associated with the member ID numbers.	301,628
Tennessee / Florida	2/28/2007	Gulf Coast Medical Center	Patient information including names and Social Security numbers was compromised when two computers went missing. 1,900 individuals were affected by a theft in Nashville, TN in November and 8,000 when another computer was stolen in Tallahassee in February.	9,900
Texas	4/26/2005	Christus St. Joseph's Hospital	Stolen computer	19,000

Texas	8/29/2006	Valley Baptist Medical Center	A programming error on the hospital's web site exposed names, birth dates, and SSNs of healthcare workers in late August. The error was fixed but it is not known how long the personal information was compromised. The affected individuals are workers from outside the hospital who provide services and bill the hospital via an online form.	Unknown
Texas	2/19/2007	Seton Healthcare Network	A laptop with uninsured patients' names, birth dates and Social Security numbers was stolen last week from the Seton hospital system. The uninsured patients had gone to Seton emergency rooms and city health clinics since July 1, 2005.	7,800
Texas	2/14/2008	Tenet Healthcare Corporation	A ex-employee worked at a Frisco, Texas, billing center for less than two years, and is confirmed to have stolen the names, Social Security numbers and other personal information of about 90 patients. The employee also had access to 37,000 other accounts.	37,000
Texas	3/10/2008	Texas Department of Health and Human Services	Information, including Social Security numbers that could be used to steal Medicaid clients' identity may have been stored on two computers stolen during a burglary. Computers could have contained personal information only on e-mails. The e-mails, however, would normally contain only an individual's case number. It is unlikely those e-mails would have listed Social Security numbers.	Unknown
Texas	8/7/2008	Harris County Hospital	A lower-level Harris County Hospital District administrator downloaded medical and financial records for patients with HIV, AIDS and other medical conditions onto a flash drive that later was lost or stolen. This may have been a violation of law. The data on the device included the patients' names, medical record numbers, billing codes, the facilities where the office visits occurred and other billing information. It also included the patients' Medicaid or Medicare numbers, which can indicate their Social Security numbers or those of their spouses.	1,200
Texas	11/1/2008	Baylor Health Care System Inc.	A laptop computer containing limited health information on 100,000 patients was stolen from an employee's car. Included were 7,400 patients whose Social Security numbers were stored on the computer.	100,000
Texas	11/7/2008	Christus Health Care	Two computer back-up tapes were stolen. Someone broke into a car in a Houston parking lot and took the tapes. The information on the tapes included patient names, Social Security numbers, demographic information, and in some cases, diagnosis codes.	Unknown
Texas	2/9/2009	Parkland Memorial Hospital	A laptop computer that may have contained the names, birthdates and Social Security numbers of 9,300 employees of Parkland Memorial Hospital was stolen.	9,300
Texas	7/1/2009	Carrell Clinic	Arlington Security Guard Arrested on Federal Charges for Hacking into Hospital's Computer System, Defendant Allegedly Posted Video of Himself Compromising a Hospital's Computer System on YouTube. The system and computers containing confidential patient information.	Unknown
Texas	1/27/2010	Methodist Hospital	Methodist Hospital notified people that someone stole a laptop from an office at the Smith Tower in the Texas Medical Center. A thief took the laptop on January 18. The computer was attached to a medical device that tests pulmonary function and contained private health information and Social Security numbers.	689

Texas	2/11/2010	University of Texas Medical Branch	The University of Texas Medical Branch has mailed letters notifying 1,200 patients that sensitive information about them had been available to a woman charged with identity theft in an unrelated case. Officials sent out the letters this week after MedAssets, which the medical branch hired to assist with billing from third-party payers, warned of a security breach by one of its employees. Law enforcement officials notified MedAssets that a former employee had been arrested and charged with identity theft. The person also was alleged to have used a stolen identity to misrepresent herself and gain employment at Georgia-based MedAssets and had been involved in other instances of identity theft. That employee is implicated in a widespread identity theft investigation involving cases from Texas to Wisconsin and losses upward of $1 million,	1,200
Utah	11/2/2006	Intermountain Health Care	A computer was purchased at a second-hand store, Deseret Industries, that contained the names, Social Security numbers, employment records, and other personal information about Intermountain Health Care employees employed there in 1999-2000.	6,244
Utah	3/13/2008	University Health Care (Utah)	A laptop and flash drive containing patient data were stolen after hours from a locked office. Data included patients' names, addresses, and in some cases, medications, health insurance policy numbers, and Social Security numbers.	4,800
Utah	6/10/2008	University of Utah Hospitals and Clinics	Billing records of 2.2 million patients at the University of Utah Hospitals and Clinics were stolen from a vehicle after a courier failed to immediately take them to a storage center. The records, described only as backup information tapes, contained Social Security numbers of 1.3 million people treated at the university over the last 16 years.	2,200,000
Virginia	9/18/2006	DePaul Medical Center, Radiation Therapy Dept.	Two computers were stolen, one on August 28 and the other Sept. 11. Personal data included names, date of birth, treatment information, and some SSNs.	100+
Virginia	1/26/2007	WellPoint's Anthem Blue Cross Blue Shield	Cassette tapes containing customer information were stolen from a lock box held by one of its vendors. Data included names and SSNs.	196,000
Virginia	2/9/2007	Radford University, Waldron School of Health and Human Services	A computer security breach exposed the personal information, including SSNs, of children enrolled in the FAMIS program, Family Access to Medical Insurance Security.	2,400
Virginia	10/19/2008	Mary Washington Hospital	A security breach in an online computer system exposed the private medical information of some of its maternity patients. Social Security numbers, phone numbers, address, insurance carrier, birth dates and doctor's names were exposed.	803
Virginia	5/4/2009	Virginia Health Data Potentially	The FBI and Virginia State Police are searching for hackers who demanded that the state pay them a $10 million ransom for the return of millions of personal pharmaceutical records they say they stole from the state's prescription drug database. A notice posted on the DHP Web site acknowledged that the site "is currently experiencing technical difficulties which affect computer and e-mail systems." Some customer identification numbers, which may be Social Security numbers, were included, but medical histories were not.	531,400
Washington	8/11/2006	Madrona Medical Group	On Dec. 17, 2005, a former employee accessed and downloaded patient files onto his laptop computer. Files included name, address, SSN, and date of birth. The former employee has since been arrested.	6,000

Washington	8/29/2006	Compass Health	Compass Health notified some of its clients that a laptop containing personal information, including SSNs, was stolen June 28. The agency serves people who suffer from mental illness.	"A limited number of people"
Washington	9/28/2006	Stevens Hospital Emergency Room via dishonest employee of billing company Med Data	A manager for the hospital's billing company, Med Data, stole patients' credit card numbers. She gave them to her brother who bought $30,000 worth of clothes and gift cards over the Internet. The woman is scheduled for sentencing in Nov. and her brother's trial is expected Jan. 2007.	30
Washington	10/25/2006	Swedish Medical Center, Ballard Campus	An employee stole the names, birthdates, and Social Security numbers from patients who were hospitalized or had day-surgeries from June 22 to Sept 21. She used 3 patients' information to open multiple credit accounts.	1,100
Washington	3/23/2007	Group Health Cooperative Health Care System	Two laptops containing names, addresses, Social Security numbers and Group Health ID numbers of local patients and employees have been reported missing.	31,000
Washington	3/23/2007	Swedish Urology Group	Three computer hard drives with personal files on hundreds of local patients including was stolen.	"hundreds"
Washington	6/4/2007	Stevens Hospital	Laptop exposed to Internet, information did include names, addresses, and Social Security numbers.The situation occurred when one of the subcontractors had a lapse in its data security procedures.	550
Washington	2/10/2008	Administrative Systems, Inc.	A desktop computer stolen from an Administrative Systems, Inc. (ASI) office in Seattle contained names and sensitive information about customers or employees of several of the firm's clients: Continental American Medical, EyeMed Vision/Kelly Services Vision, and Jefferson Pilot Financial Dental. Personal details may have included name, date of birth, mailing address, and Social Security number, depending on the service being provided.	Unknown
Washington, DC	5/6/2006	US Dept of Veteran's Affairs	A data tape disappeared from a VA facility in Indianapolis, IN that contained information on legal cases involving U.S. veterans and included veterans' Social Security numbers, dates of birth and legal documents.	16,500
Washington, DC	5/22/2006	US Dept of Veteran's Affairs	On May 3, data of all American veterans who were discharged since 1975 including names, Social Security numbers, dates of birth and in many cases phone numbers and addresses, were stolen from a VA employee's home. Theft of the laptop and computer storage device included data of 26.5 milliion veterans. The data did not contain medical or financial information, but may have disability numerical rankings.	28,600,000
Washington, DC	7/25/2006	Georgetown University Hospital	Patient data was exposed online via the computers of an e-prescription provider, InstantDx. Data included names, addresses, SSNs, and dates of birth, but not medical or prescription data. GUH suspended the trial program with InstantDX.	23,000
Washington, DC	6/2/2008	Walter Reed Army Medical Center	Sensitive information on patients at Walter Reed Army Medical Center and other military hospitals was exposed in a security breach. The computer file that was breached did not include information such as medical records, or the diagnosis or prognosis for patients, but may have included names, Social Security numbers, birth dates as well as other information.	1,000
West Virginia	1/20/2009	Kanawha-Charleston Health Department	People who received flu shots from the agency since October, are being warned that their personal information may have been stolen by a former department temporary worker. Information included their names, social security numbers, addresses and other personal information.	11,000

Wisconsin	12/2/2006	Gundersen Lutheran Medical Center	A Medical Center employee used patient information, including SSNs and dates of birth, to apply for credit cards in their names. As patient liaison, her duties included insurance coverage, registration, and scheduling appointments. She was arrested for 37 counts of identity theft, and was convicted of identity theft and uttering forged writing, according to the criminal complaint.	Unknown
Wisconsin	2/19/2007	Social Security Administration	Files of disability applicants containing Social Security numbers, addresses, phone numbers of family members, dates of birth and work history, and detailed medical information were lost/stolen when a telecommuting employee abandoned them in a locked filing cabinet at home after a threat of domestic violence. Several of the files were mailed back to the local SSA office months later; others were found in a dumpster recently, and four were never recovered.	13
Wisconsin	1/8/2008	Wisconsin Department of Health and Family Services	Social Security numbers were printed on about 260,000 informational brochures sent by a vendor hired by the state, Electronic Data Systems Inc. (EDS), to recipients of SeniorCare, BadgerCare and Medicaid. The company agreed to pay $250,000 to the state for the mistake, as well as paying for an identity theft monitoring service for the affected individuals, for a total of about $1 million..	260,000
Wisconsin	11/25/2009	Aurora St. Luke's Medical Center	6,400 people who were in-patients at St. Luke's are being warned that their name, Social Security number and other information may have landed in the hands of thieves, due to a stolen laptop computer. All of the at-risk individuals were cared for there at some point by a hospitalist, a physician other than the patient's primary care doctor, who works for an independent physician group called Cogent Healthcare. The computer was stolen from a locked office in a secure physician office building that's located adjacent to the hospital, and the computer belongs to an employee of Cogent Healthcare of Wisconsin.	6,400
Wyoming	2/6/2010	Wyoming Department of Health	The personal information of about 9,000 children in the state's children's health insurance program could have been exposed on the Internet. The error resulted in the names, birthdays, Social Security numbers, addresses and phone numbers of Kid Care CHIP participants being accessible on an unsecured Web page for months.	9,000
			Total:	45,258,468 +

*Source Privacy Rights Clearinghouse, http://www.privacyrights.org/ar/ChronDataBreaches.htm#2006 (last visited Feb. 2, 2010).

"The list is a useful indication of the types of breaches that occur, the categories of entities that experience breaches, and the size of such breaches. But the list is not a comprehensive listing. Most of the information is derived from the Open Security Foundation list-serve which is in turn derived from verifiable media stories, government web sites/pages, or blog posts with information pertinent to the breach in question. Many breaches (particularly smaller ones) may not be reported. If a breached entity has failed to notify its customers or a government agency of a breach, then it is unlikely that the breach will be reported anywhere. Most of the breaches summarized below on this page have been obtained from the Open Security Foundation list-serve. The Open Security Foundation's DataLossDB.org(www.datalossdb.org) offers a free e-mail list-serve on the latest breaches. To subscribe to DataLoss, send a message to:dataloss-subscribe@datalossdb.org. The DataLossDB.org page includes a search engine and news articles for the breaches listed below, and also provides an open source database of its data breach records. It is a flat comma-separated value file that can be imported into a database or spreadsheet program for your own data analysis. Visit http://datalossdb.org/download."

Tab 4

Essential Elements For Protecting The Patient's Right To Health Information Privacy And Access To Quality Psychotherapy.

I. Recognize that individuals *have* a right to health information privacy that will be preserved and protected in an electronic health information system.

II. Adopt the commonly accepted definition of "health information privacy".

III. Expressly preserve the patient's right to privacy under the psychotherapist-patient privilege and include this in the notice of rights to patients.

IV. Include the patient's right of authorization for disclosure of "psychotherapy notes" in the notice of privacy practices.

V. Allow for the "segmentation and protection from disclosure" of sensitive identifiable mental health information "with the goal of minimizing the reluctance of patients to seek care (or disclose information about a condition) because of privacy concerns".

VI. Clearly state in regulations that "minimum necessary" determinations are to be "consistent with, and not override, professional judgment and standards.

VII. The patient's right to pay privately to protect the privacy of mental health information must be preserved.

COALITION FOR PATIENT PRIVACY

August 3, 2009

Dr. David Blumenthal
Office of the National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Ave, SW
Suite 729D
Washington, DC 20201

Re: Comments to the HIT Policy Committee on the July 16, 2009 meeting

Dear Dr. Blumenthal and Members of the Committee:

The Coalition for Patient Privacy (the Coalition) is the leading voice of consumer organizations working to protect patient privacy and encourage adoption of Health IT, representing millions of Americans. We are a diverse, multi-partisan and collaborative group united by the effort to prevent discrimination and preserve the ethical basis of the health care system.

The Coalition's three central tenets for Health IT are Accountability, Control of Personal Information and Transparency, "A.C.T. for Privacy". The Coalition worked tirelessly in 2008/2009 to lead the grassroots effort to ensure historic privacy protections were included along with the $19 billion federal investment in Health IT as part of the American Recovery and Reinvestment Act (ARRA).

Thank you for the opportunity to comment on the last HIT Policy Committee (the Committee) meeting held July 16, 2009. We comment today to raise concerns regarding the public's lack of opportunities to provide meaningful feedback to this body, the need to protect and enable patient control over protected health information at the beginning of this process, and the approved "meaningful use" matrix.

<u>Public Comment & Participation:</u>

We appreciate the Committee's attempts to invite public comment on these critical matters. We also appreciate the incredibly restrictive timeframes in place. Nevertheless, we urge the Committee to allow additional time and opportunity to hear and incorporate the public perspective. It is incredibly complicated and difficult for the public to participate in meaningful ways in this important policy making process.

The Committee has access to a tremendous wealth of expertise from the health care and information technology industries. At the end of the day, it is *the patient* that opts to share his/her personal information with a provider, and it is *the patient* that must be assured electronic health record systems can be trusted. In the "Overview of Public Comments" presentation summarizing the 792 comments received on "Meaningful Use" criteria there was

no mention of any concerns or proposals offered by any consumer or health privacy advocacy organizations. This is a striking omission from the presentation on the comments. While we will certainly do our part to ensure you hear from a large constituency, the Committee's policies will fall short of public expectations if it does not discuss any public comments from patients.

At times, the interests of the health care, HIT, research, insurance, pharmaceutical and data mining industries are in direct conflict with Americans' longstanding legal and ethical rights to control personal health information. Without additional consumer and patient engagement, expecting this process to protect consumers is like expecting foxes to design hencoops that chickens will trust. Similar to the auto, banking, and securities industries, the HIT, pharmaceutical, insurance, and healthcare industries will never add consumer protections willingly. They will always claim consumers' privacy rights are impossible, too complex, too expensive, or unnecessary to protect. However, we believe their claims are spurious and that the technical capacity and federal policy precedents are available now to add the essential consumer privacy protections to the "meaningful use" criteria and quality matrices.

Recommendations:

1) When matrices and recommendations are presented to the Committee as a whole, such information must be made available to the public a minimum of two (2) days prior. Alternatively, time must be allotted to receive public comment BEFORE the Committee approves such recommendations, so that the Committee could better understand and aggressively debate consumers' proposals. We understand formal requests for public comment published in the Federal Register are part of the formal rulemaking process that will take place after the Committee makes final recommendations. Nevertheless, we believe that our proposals and concerns should be openly addressed and debated during the deliberative stage of the Committee's work. Even an informal solicitation of public comments prior to decision making would greatly improve this process.

2) We urge you to work directly with our broad–based Coalition and any other consumer health privacy advocacy organizations accountable to the public.[1]

<u>Greater Attention to Protecting and Enabling Privacy</u>

Generally speaking, the discussions from this Committee are driven from an industry (health care and information technology) point of view primarily. Providers' points of view are secondary in the process, and patients seem to fall into the mix last – the caboose -- if at all. We strongly urge a complete reversal of these perspectives. *First, the patient's needs and rights must guide policy. Second, these needs and rights must be addressed on the front end, not the back.*

The Coalition hears from our far-reaching constituencies that having control over who can access and use their most personal information, or privacy, is their paramount concern. We

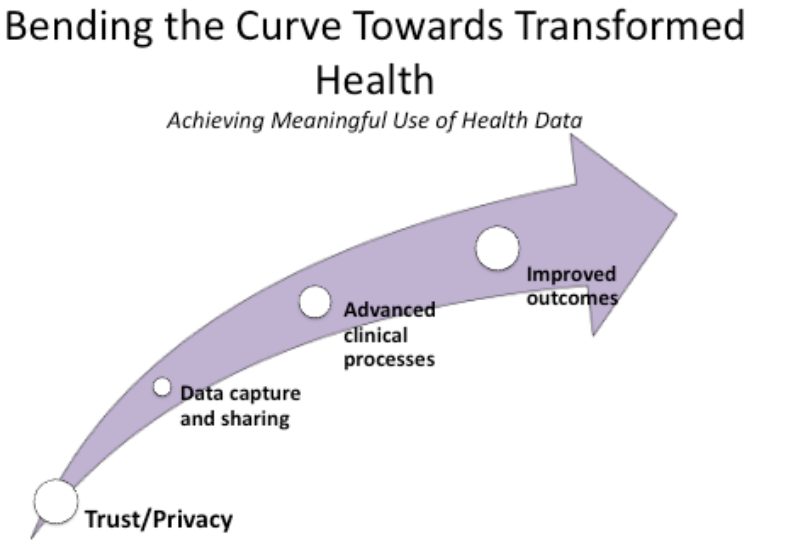
[1] We note the language creating the HIT Policy Committee requires it to "serve as a forum for broad stakeholder input" and it "shall ensure an opportunity for the participation …of outside advisors, including individuals with expertise in the development of policies for the electronic exchange and use of health information, including in the areas of health information privacy and security. . . "

cannot reach the ultimate vision for HIT, nor meet the key goals to improve quality, safety and efficiency, engage patients and families, improve coordination, improve public health and reduce disparities, and ensure privacy and security protections, if we begin with what is easy rather than what is crucial. While ensuring privacy may be challenging, it is workable and more importantly, essential.

First, while we certainly appreciate the need for gradual implementation, the key technology features needed to ensure public trust, items such as segmentation, consent management and audit trails need to be addressed now. Likewise, policy matters such as how Americans can control their information and how they can opt-out of systems are not a matter that can or should be dealt with later. Clearly Committee member Dr. Sweeney heard this concern, as did other members.

Second, the issue of privacy is raised countless times during the Committee's meetings; but we have yet to see any comprehensive or cross-cutting attention given to privacy in the Committee's recommendations. The few privacy measures will not be addressed until 2015. Further, the Committee does not have an agreed upon definition of privacy. "Privacy" is an easily used term, often mixed with "security" or "confidentiality" causing confusion and making it impossible to measure progress. Privacy is essential for quality healthcare; it should be a quality metric measured as part of the "meaningful use" criteria.

Finally, we note that quality healthcare depends on privacy[2]. In the slide used for the Meaningful Use Workgroup Presentation entitled, "Bending the Curve Towards Transformed Health", the starting point for the arrow in the slide is "data capture and sharing." Again, having TRUST is essential before patients are willing to give providers any data to capture. Trust and privacy (and security) need to be the starting point; we suggest an alternative approach:



[2] "The **entire health delivery system** is based upon the willingness of the individual to trust a health care practitioner sufficiently to disclose to the practitioner the most intimate details of his or her life." "An assurance of privacy of health information is **necessary to secure effective, high quality health care.**" 65 Fed. Reg. at 82,467

Accurate and complete information cannot be obtained by force. We know from the California HealthCare Foundation's National Consumer Health Privacy Survey (2005) that 12.5% of the population avoids their regular doctor, asks doctors to alter diagnoses, pays privately for a test, or avoids tests altogether due to privacy concerns. If we do not restore patient control over PHI, we can expect electronic health data to have error and omission rates of 12.5 % or more. The breakthroughs and benefits possible with technology-enhanced research will never be reached with such a high rate of errors and omissions.

The lack of privacy drives patients away from doctors. We know from HHS' findings that every year 600,000 people refuse early diagnosis and treatment for cancer and 2,000,000 avoid treatment for mental illness because of fears their treatment will not be private[3]. The lack of privacy causes death, suffering, and, most importantly, bad outcomes. This is happening right now and will only get worse as we migrate to electronic health records. Given that 68% of the public have little confidence that electronic health records will remain confidential, the Committee needs to act immediately to ensure the public's fears are alleviated by policies and standards that ensure EHRs can be trusted.[4]

Recommendations:

1) The Committee should adopt a definition of privacy. We urge adoption of the NCVHS definition of health information privacy: "*individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data."*

2) Ensure that <u>the patient perspective</u> is prominently represented and, in fact, heard in <u>each</u> of the three workgroups. The Coalition is happy to assist the Committee with feedback for each workgroup as recommendations are developed to ensure privacy is addressed.

3) Reject any recommendations that call for collecting all "comprehensive data available" and to "record all available data" without first laying the groundwork for privacy and ensuring consumer control and informed consent.

<u>Approved "Meaningful Use" Matrix</u>

In addition to our previous comments about meaningful use, we note that we were encouraged to see among the 2011 objectives for Privacy and Security in the Meaningful Use Matrix (7.10.09) compliance with the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information (Framework).

This Framework includes the strong privacy principle that "*Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information."* Compliance with the Framework is stated as a 2011 objective. Yet there does not appear to be any actual requirement for this key privacy policy, nor any way to verify compliance. We applaud many of

[3] 65 Fed. Reg. at 82,779 and 82,777.

[4] See the survey data from the Employee benefit Research Institute and Mathew Greenwald & Associates presented by the Privacy and Security Work Group to the HIT Standards Committee on July 21, 2009

the principles and policies set forth in the Framework but note that they are not all being addressed as part of the “meaningful use” matrix.

The key critical function needed in every EHR to enable "meaningful use" of EHR data is the ability of patients to control the uses and disclosures of all protected health information (PHI). We recommended previously that the Committee adopt existing open source technology that enables detailed control over disclosures as a baseline model or floor for consent technologies. The open source technology we recommended has the added advantage of enabling robust segmentation, so adoption of the functions in this technology as a minimum standard for privacy and segmentation would allow these two critical consumer protections to be quickly implemented as requirements for “meaningful use” in EHRs. We believe that ultimately, certification of systems for “meaningful use” that do not require consumer control over data fail to meet public’s expectations.

With regard to measures and objectives for the accounting of disclosures for treatment, payment and healthcare operations, we remind the Committee that ARRA requires no later than 2013 for EHRs purchased after January 1, 2009 audit trails be in place. For these “new” EHRs, an audit trail is required by 2011, and no later than 2013. As such, it is essential that the Committee develop the needed policies now.

Acknowledging the time needed for implementation, we also urge the Committee to recommend policies that will guide the development of new privacy-enhancing technologies. Early attention is needed for the successful implementation of segmentation and consent management features. If these protections are placed on the backburner, EHRs will be purchased and used over the next four years without those critical features and make retrofitting for privacy a burden.

Recommendations:

1) Include compliance with the policies and principles in the Nationwide Privacy and Security Framework as a 2011 measure so that these principles are both required and verified. The Committee could delay some portions of this framework until 2013, but 2011 should be the goal.

2) Add minimum standards for basic consent management tools to the “meaningful use” criteria. We recommend that EHRs must include consent and segmentation capabilities at least as detailed and specific as those in the open source electronic consent controls developed by the NDIIC, as recommended in our previous comments.

3) Add consumer control over PHI in EHRs as a “meaningful use” quality measure, tracked and improved over time.

4) Include objectives for audit trails, segmentation and consent management in 2011 and 2013 as part of the meaningful use matrix. Even if these objectives are not required for federal funds (for segmentation and consent management), the steps towards 2015 implementation should be articulated as early as possible.

Our Coalition is committed to working closely with you and the HIT Policy Committee to ensure patients and consumers are represented and that we achieve progress by protecting privacy. Thank you for your time and consideration. Please do not hesitate to contact us.

Sincerely,

The Coalition for Patient Privacy

American Association of People with Disabilities
American Civil Liberties Union
Center for Digital Democracy
Clinical Social Work Association
Consumer Action
Electronic Frontier Foundation
Electronic Privacy Information Center
Just Health
Multiracial Activist
National Center for Transgender Equality
National Coalition for LGBT Health
National Coalition of Mental Health Professionals & Consumers
Patient Privacy Rights
Private Citizen
Tolven, Inc.
U.S. Bill of Rights Foundation

For more information, please contact:

Ashley Katz
Executive Director, Patient Privacy Rights
akatz@patientprivacyrights.org (512) 732-0033