MYTHS, FACTS AND LAW ABOUT HEALTH IT AND THE RIGHT TO HEALTH INFORMATION PRIVACY

Revised January 27, 2008

The American Psychoanalytic Association, one of the nation's oldest and most respected mental health professional associations, offers these Myths, Facts and Law About Health Information Technology and the Right to Health Information Privacy to the Obama Administration and the 111th Congress in the interest of (1) preserving access to effective mental health care, (2) protecting one of Americans' most cherished and fundamental rights, and (3) creating the trust that many, including the Clinton and Bush Administrations, now consider to be essential for public acceptance of a national electronic health information system.

In offering these carefully substantiated facts and law, APsaA hopes to assist the Obama Administration in abandoning the "truly poisonous legacy of the past eight years"[1] in which facts and law that were inconvenient to corporate special interests were ignored, distorted and suppressed. This is the third update of this document and, as in the past, each statement of fact and law is carefully corroborated to distinguish these "Myths and Facts" from those that may have been disseminated by other groups supported by large corporate "stakeholders" that disguise essentially unsupported personal opinion as "facts". These facts and law are offered in the hope that the Obama Administration and the new Congress will take a "reality-based" approach to the design and implementation of health IT legislation that gives priority to the interests of the one group of "stakeholders" whose support, trust and confidence is indispensable to the health care system and successful implementation of health IT—the patients.

In considering these myths and facts and legislative options, we suggest that Congress and the Obama Administration continuously ask two simple questions—(1) what would we, as patients want and (2) can any impartial person seriously believe that most Americans would be willing to relinquish their right to health information privacy in order to have access to an electronic health information system? Of course, this is a false choice since it should be possible to design a health IT system that preserves the patient's right to privacy rather than eliminates it.

1. **Myth—A right to health information privacy in health IT legislation would be a new concept.**

   Fact—Congress has expressly found that Americans have a right to privacy for personal information about themselves that is a "personal and

[1] Bring On the Reality-Based Community, Newsweek, p. 36 (Nov. 17, 2008).

fundamental right protected by the Constitution of the United States".[2] The right to privacy in this country is "older than the Bill of Rights".[3] This "reasonable expectation" of privacy for health information has been recognized repeatedly by courts at every level of the federal judiciary.[4] In fact, the right to privacy for highly personal health information is now so well established that no reasonable government official could be unaware of it.[5]

The right to health information privacy is also found in the physician-patient privilege recognized in 43 states[6], and in the psychotherapist-patient privilege recognized in all 50 states and the District of Columbia and in Federal common law.[7] The Department of Health and Human Services (HHS) has acknowledged that the privacy of highly personal information "is a fundamental right."[8]

The right to privacy of personal information including health information is recognized under the tort law or statutory law of all 50 states.[9] Ten states (Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington) include a specific right to privacy in their state constitutions. The Supreme Courts in other states such as Tennessee and Texas, have found that a right to privacy is implied in the state constitution.[10] The standards of medical and professional ethics adopted by virtually all segments of the medical and mental health profession recognize and protect the patient's right to health information privacy.[11] The Supreme Court of New Jersey has recently recognized that individuals have a right to privacy for information transmitted over the internet.[12]

The National Committee on Vital and Health Statistics (NCVHS) has found: "Privacy and confidentiality are neither new concepts, nor

---

[2] Pub. L. 93-579, section 2(a)(4).
[3] Griswold v. Connecticut, 381 U.S. 479, 516 (1987).
[4] 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).
[5] Gruenke v. Seip, 225 F.3d 290, 302-03 (3rd Cir. 2000). See also, Sterling v. Borough of Minersville, 232 F.3d 190, 198 (3rd Cir. 2000).
[6] See, e.g., Northwest Mem. Hosp. v. Ashcroft, 362 F.3d 923 (7th Cir. 2004).
[7] Jaffee v. Redmond, 116 S.Ct. 1923 (1996).
[8] 65 Fed. Reg. at 82,464.
[9] HHS Finding, 65 F.R. 82,464 (Dec. 28, 2000).
[10] Planned Parenthood of Middle Tenn. v. Sundquist, *38 S.W.3d 1, 6, n. 3 (Tenn. 2000).*

[11] See, e.g., Principles of Medical Ethics, American Medical Association, "Our AMA policy is that where possible, informed consent should be obtained before personally identifiable health information is used for any purpose." H-315.978 Privacy and Confidentiality. See also attached ethics standards.
[12] "New Jersey Justices Call E-Privacy Surfers' Right: Ruling on Warrant Trumps Top U.S. Court's Decisions", The Star-Ledger (April 22, 2008).

absolutes. Since the time of Hippocrates physicians have pledged to maintain the secrecy of information they learn about their patients disclosing information only with the authorization of the patient or when necessary to protect an overriding public interest, such as public health. Comparable provisions are now contained in the codes of ethics of virtually all health professionals."[13]

2. Myth—The right to health information privacy is not important for quality health care.

Fact—HHS has found that "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 providers."[14] If the privacy of sensitive health information is not recognized and protected, the information will simply not exist because the patients will not disclose it to their practitioners.[15] So, "privacy is necessary to secure effective high quality health care."[16]

3. Myth—An "interoperable" electronic health information system poses no new or additional threat to health information privacy.

Fact—The use of interoperable electronic health information systems for transmitting and storing identifiable health information creates the following threats to health information privacy that are unprecedented in the history of medicine:

A. The identifiable health information of millions of individuals can be improperly disclosed to other individuals "in a matter of seconds"[17];

B. 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[18]; and

C. When an individual's health information privacy is breached electronically, it can never be restored.[19]

---

[13] Finding of the National Committee on Vital and Health Statistics, letter to Secretary Leavitt, p. 3 (June 22, 2006).
[14] HHS Finding, 65 Fed. Reg. at 82,467.
[15] HHS Finding, 65 Fed. Reg. at 82,468; Jaffee v. Redmond, 116 S.Ct. 1923, 1929 (1996).
[16] HHS Finding, 65 Fed. Reg. at 82,467.
[17] 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).
[18] "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).
[19] HHS Finding, 65 Fed. Reg. at 82,465.

In fact, Congress has found "the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information."[20] More recently, the increasing risk to health information privacy posed by electronic information systems has been recognized by a Presidential Task Force, and the Government Accountability Office.[21]

The privacy of **at least 236 million electronic records** has been reported violated or compromised since January 1, 2005. The privacy of **at least 42,046,667 electronic health records** has been reported breached or compromised over that period of time.[22] The actual number of electronic health records whose privacy has been breached or compromised could be double that number since a recent survey showed that nearly half of such breaches are not reported, and the HIPAA Privacy Rule does not require breaches to be reported.[23]

4. Myth—Electronic health information systems are secure.

Fact—A recent industry sponsored survey showed that all of the electronic health information systems currently in use are "severely at risk of being hacked".[24] A Presidential Cybersecurity Task Force has determined that attacks and vulnerabilities on electronic information systems are growing by 20% a year and cannot be addressed by the current "patching" approach.[25] HHS has found that "[T]here is no such thing as a totally secure [HIT] system that carries no risks to security."[26] The Office of Management and Budget has found that **the number of attacks on federal electronic information systems increased 60%** between 2006 and 2007.[27]

---

[20] Pub. L. 93-579, section 2(2).
[21] "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.").
[22] Privacy Rights Clearinghouse, http://www.privacyrights.org/ar/ChronDataBreaches.htm.
[23] "Nearly Half of Data Breaches Not Disclosed: Report", Modern Healthcare Online (April 8, 2008); 45 C.F.R. 164.530.
[24] "Electronic Records at Risk of Being Hacked, Report Warns," SearchCIO.com (Sept. 19 2007).
[25] "Cyber Security: A Crisis in Prioritization", supra at 10-12.
[26] HHS Finding, Security Rule, 68 Fed. Reg. at 8346 (Feb. 20, 2003).
[27] "Feds Losing War On Information Security, Senators Told," Govexec.com (March 13, 2008) http://www.govexec.com/story_page.cfm?articleid=39518&dcn=e_gvet

5. **Myth—Protection of the individual's right to health information privacy is not essential for public acceptance of a national electronic health information system.**

   Fact—NCVHS has determined that: "In an age in which electronic transactions are increasingly common and security lapses are widely reported, public support for the NHIN [national health information network] 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. **The health care industry must commit to incorporating privacy and confidentiality protections so that they permeate the entire health records system."**[28]

   According to HHS: "Unless public fears are allayed, we will be unable to obtain the full benefits of electronic technologies. The absence of national standards for the confidentiality of health information has made the health care industry and the population in general uncomfortable about this primarily financially-driven expansion in the use of electronic data."[29]

   Even the Bush Administration has finally recognized: "The growing computerization, exchange and analysis of patient data offer the potential to improve the quality of care and reduce costs and medical errors, but those benefits won't be fully realized until privacy concerns are effectively addressed."[30]

6. **Myth—The public is not concerned about the threat that an electronic health information system poses to health information privacy.**

   Fact—The Government Accountability Office (GAO) has found that "…70 percent of Americans are concerned that an electronic medical record system could lead to sensitive medical information being exposed because of weak security, and 69 percent are concerned that such a system would lead to more personal health information being shared without the patient's knowledge."[31]

7. **Myth—The right to health information privacy means protecting identifiable health information from theft or improper disclosure.**

---

[28] Finding of the National Committee on Vital and Health Statistics, letter to HHS Secretary Leavitt, p. 3 (June 22, 2006).
[29] HHS Finding, 65 Fed. Reg. at 82,466.
[30] Statement of HHS Secretary Michael Leavitt, HHS News (Dec. 15, 2008).
[31] GAO Finding, "Health Information Technology, supra note 21, at 9-10.

Fact—NCVHS has determined that health information privacy means "an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data." Confidentiality means "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."[32] According to HHS, "the right of privacy is: 'the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated.'"[33] The courts have defined privacy as "control over knowledge about one's self."[34] And the most often quoted definition is that privacy is "the right to be let alone".[35] So the accepted definition of health information privacy includes the individual's right to control the disclosure of his or her health information.

8. Myth—The right to health information privacy is recognized and protected in the HIPAA Health Information Privacy Rule.

Fact—Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires the Secretary of HHS to set forth in regulation "the rights that an individual who is the subject of individually identifiable health information should have."[36] However, **the right to health information privacy is not among the "individual rights" recognized by the Rule.**[37]

The Original HIPAA Health Information Privacy Rule implicitly recognized the individual's right to health information privacy by requiring consent for the use and disclosure of identifiable health information in routine situations broadly defined as treatment, payment and health care operations.[38] However, in 2002, that implicit right was eliminated and "replaced" by federal "regulatory permission" for all covered entities to use and disclose any individual's identifiable health information for the same broadly defined purposes of treatment, payment and health care operations.[39] The HIPAA Health Information "Privacy" Rule was thereby converted from a rule that guaranteed a broad right to health information privacy to one that broadly eliminated that right.

---

[32] Definitions adopted by the National Committee on Vital and Health Statistics from the Institutes of Medicine, letter to HHS Secretary Leavitt, p. 2 (June 22, 2006).
[33] HHS Finding quoting "Who Knows: Safeguarding Your Privacy in a Networked World", A. Cavourkian, D. Tabscott, Random House (1995), 65 Fed. Reg. at 82,465.
[34] U.S. v. Westinghouse, 638 F.2d 570, 577, n. 5 (3rd Cir. 1980).
[35] "The Right to Privacy," L. Brandeis and S. Warren, 4 Harv. L. Rev. 193 (1890)
[36] 42 U.S.C. 1320d-2 note.
[37] 45 C.F.R. §164.520(b)(1)(iv).
[38] 45 C.F.R. §164.506, 65 Fed. Reg. at 82,810 (Dec. 28, 2000).
[39] 45 C.F.R. §164.506(a), 67 Fed. Reg. at 53,211 (Aug. 14, 2002).

9. **Myth—HIT legislation, even without protections for the right to health information privacy, is necessary to save 98,000 lives annually and avoid suffering due to medical errors.**

Fact—The lack of adequate privacy protections in a national health IT system could well cause more deaths and injuries than it would prevent. According to HHS, nearly **600,000 Americans each year do not seek earlier treatment for cancer** due to privacy concerns.[40] As a result of these concerns, cancer victims "may ultimately face a more severe illness and/or premature death." This delay in seeking cancer treatment costs the country an estimated **$1.6 billion each year**. Increasing the confidence of individuals in the privacy of their medical information "would encourage more people with cancer to seek cancer treatment earlier, which would increase cancer survival rates".

HHS has further found that more than **2 million Americans each year fail to seek treatment for mental illness** due to privacy fears.[41] This untreated mental illness **costs the nation between approximately $500 million and $800 million each year**. Adequate privacy protections would reduce the suffering and loss associated with untreated mental illness.

HHS has also found that many Americans do not report or seek treatment for **sexually transmitted diseases** due to privacy concerns.[42] Failure to treat sexually transmitted diseases can result in "expensive fertility problems, fetal blindness, ectopic pregnancies, and other reproductive complications." In addition, earlier treatment "translates into reduced spread of infections." The Centers for Disease Control and Prevention has recently found that 1out of 4 teenage girls in America suffer from a sexually transmitted disease.[43]

HHS has also concluded that the adverse impact of privacy concerns on the treatment of the above diseases would likely occur with "**any health condition, including relatively minor conditions.**" HHS also concluded that "some individuals might be concerned with maintaining privacy even if they have no significant health problems because it is likely that they will develop a medical condition in the future that they will want to keep private."[44]

A recent report by the RAND Corporation (the same organization that conducted in initial study on the benefits of health IT) found that **300,000 soldiers returning from the wars in Iraq and Afghanistan suffer from**

[40] 65 Fed. Reg. at 82,777.
[41] 65 Fed. Reg. at 82,779.
[42] 65 Fed. Reg. at 82,778.
[43] "1 in 4 Teen Girls Has At Least One STD", Associated Press (March 11, 2008).
[44] 65 Fed. Reg. at 82,777.

Post-Traumatic Stress Disorder (PTSD) but less than half seek treatment for the reason that "if they received treatment, it would not be kept confidential and would constrain future job assignments and career advancement."[45] A "key finding" of the RAND Corp. report was that "[m]any of the most commonly identified barriers to getting needed mental health treatment could be **reduced if service members had access to confidential treatment."[46] The cost of the avoidance of such is estimated to range from $4 billion to $6 billion** "depending on how we account for the costs of the lives lost to suicide." [47]

So the failure to include privacy protections in health IT legislation is likely to exact a cost in lost lives and unnecessary suffering that is much higher than any potential savings accruing from health IT.

Further, the extent to which health IT will reduce medical errors and save lives is unclear. First, the 98,000 avoidable deaths attributed to medical errors is based on an Institutes of Medicine report in 2000 of studies in two hospitals, one in 1984 and one in 1992. The IOM report actually projected a range of possible preventable deaths ranging from 44,000 to 98,000. There has been significant question concerning whether the medical errors were actually "preventable" and whether the preventable errors actually led to the deaths of the patients.[48] For example, one recent review of the IOM study reached the following conclusion:

> "The principal argument for the push to adopt CPOE has been the promise of lifesaving benefits. While we believe that CPOE has great potential to improve the health care process, we have to agree with Berger and Kichak's position that **a convincing case for lifesaving benefits has not been made.** As Berger and Kichak point out, the keystone for these arguments—namely the Institute of Medicine's (IOM's) claim of 44,000 top 98,000 deaths due to medical errors—**crumbles on close inspection**."[49]

The IOM study ignored the fact that **"the patients with adverse events had a death rate no different than the death rate (13.8%) of the target population from which they were drawn."[50]**

---

[45] "Invisible Wounds of War", The RAND Corp., p. 436 (2008).
[46] RAND Corp. report at 436.
[47] RAND report at 438.
[48] "How Many Deaths Are Due to Medical Error? Getting the Number Right," Effective Clinical Practice (Nov./Dec. 2000) ("…Americans do not have a credible estimate of the number of deaths caused by medical error. Without such an estimate, it is impossible to make an informed policy decision about how many of our limited resources should be devoted to reducing errors as opposed to other competing health needs.").
[49] "Physicians, Information Technology, and Health Care Systems: A Journey, Not a Destination," C. Clement, M.D., et al., J. Am. Med. Inform. Assoc., 11:121-124 (March/April 2004).
[50] Id.

There must further be a question of how many, if any, of these medical errors even if they led to the death of the patients in 1984 and 1992 could have been prevented by an electronic health information system. The IOM study does not address that.

Recent studies have shown that electronic health information systems may add other errors.[51] And some recent studies have simply not shown that electronic medical records inevitably produce higher quality care.[52] The potential benefits of a health IT system simply do not warrant implementing such a system without the privacy protections that the history of medicine shows is essential for quality health care.

For more information, contact:

Jim Pyles, Counsel
American Psychoanalytic Association

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

[51] "Veterans Exposed to Incorrect Drug Doses," Associated Press (Jan. 14, 2009); "Not Quite Fail Safe: Computerizing Isn't a Panacea for Dangerous Drug Errors, Study Shows," The Washington Post (March 22, 2005)

[52] "Electronic Medical Records and Diabetes Quality of Care: Results From a Sample of Family Medicine Practices," Annuals of Family Medicine (May/June 2007) (Practices using EMRs produced worse results in care of diabetes patients.)