

**To: Senate Health, Education, Labor and Pensions Committee Staffs**

**From: Jim Pyles, Counsel  
American Psychoanalytic Association**

**Re: Comments and recommendations on draft  
“Wired for Health Care Quality Act”**

**Date: June 4, 2007**

**I. In general—the need for privacy principles and hearings**

The American Psychoanalytic Association wishes to express its appreciation for the opportunity to provide comments on the draft “Wired for Health Care Quality Act”. We sincerely hope that our comments and recommendations will be helpful in crafting a bill that, in fact, will preserve and enhance the quality of health care and promote the establishment of a national health information technology system that the public will trust and use.

**A. The Positive Features of the Bill**

We are especially appreciative of the references in the draft to protecting or ensuring privacy and security, the provisions for notifying patients when their personal health information is “wrongfully disclosed” and requirement for an “audit record” of each individual that has gained access to a patient’s electronic health information. We also support funding the development of health IT systems through federal and state grants and loans rather than through additional exemptions to the anti-kickback laws.

**B. The Negative Features of the Bill**

We believe that the bill, as currently drafted, establishes a process which could eliminate the right to health information privacy that most citizens and practitioners believe is essential for quality health care, particularly in the area of mental health care.

For example, the bill does not recognize or preserve the patient’s right to health information privacy or the psychotherapist-patient privilege that has been recognized in all 50 states and the District of Columbia and at the federal level. The terms “privacy and security” are undefined, so it is not clear what is being “protected” or “ensured”.

It establishes two committees (the Partnership for Health Care Improvement and the American Health Information Community) which are charged with recommending standards to the Secretary of HHS for the implementation of a nationwide interoperable health information technology

system. Consumers or patient organizations, however, are out-numbered by at least 2-1 on those committees by organizations that are likely to have an interest in eliminating the patient's right to health information privacy.

While such standards adopted by the Secretary are to be published in the Federal Register, there does not appear to be any opportunity for public comment. Over the past three years, the Department of HHS has exhibited a well-documented lack of commitment to protecting the patient's right to health information privacy. On March 16, 2006, the House Government Reform Committee awarded HHS an "F" for its performance in protecting the privacy of electronic health information in both 2004 and 2005. On January 10, 2007, the Government Accountability Office found that HHS had not established a strategy for integrating key privacy protections into its electronic health information initiatives. "Health Information Technology: Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy", GAO-07-238. Thus, it would appear essential for Congress to provide minimum privacy principles to guide the Secretary's discretion if the patient's traditional right to health information privacy is to be preserved.

Moreover, the Partnership and the Community are not required to take into account the common elements of the patient's right to privacy reflected in Constitutional common law, standards of professional ethics, the physician-patient and psychotherapist-patient privilege in federal and state statutory and common law as well as state tort and contract statutory and common law. So the rights of the public and the patients, who have the most at stake in this process, are relegated to minority status or not mentioned at all.

The bill also relies on the HIPAA statute and regulations for "ensuring privacy and security", but neither the HIPAA statute or regulations recognize the patient's right to health information privacy, and the HIPAA privacy regulations permit the broad use and disclosure of patients' identifiable health information to millions of covered entities and their business associates for routine purposes without notice of the disclosures, without the patients' consent, and even over the patients' objection. Even HHS has conceded that the standards in the HIPAA Privacy Rule were never intended to be a national "best practices" standard, and the National Committee on Vital and Health Statistics (NCVHS) has concluded that HIPAA was never designed to establish privacy protections for a national electronic health information system such as contemplated in this draft bill. 65 Fed. Reg. at 82,471; 67 Fed. Reg. at 53,212; NCVHS letter to Secretary Leavitt. P.9 (June 22, 2006).

Even the requirements for notice to patients of wrongful disclosures would appear to be undermined by the provision for a GAO report concerning the "necessity and workability" of such notice. Of course, the requirement for notice of "wrongfully disclosed" information will be completely dependent upon the

standards establishing permitted disclosures recommended by the Partnership and the Community and adopted by the Secretary.

In short, the draft implies that the interests in health care quality and privacy are somehow conflicting interests that must be “balanced”. In fact, HHS found in issuing the Original HIPAA Privacy Rule preserving the right of consent in routine situations, that “privacy is necessary to secure effective, high quality health care.” 65 Fed. Reg. at 82,467. While HHS also noted that at times it is necessary to balance the individual’s needs and rights against the needs and rights of society as a whole, the Supreme Court expressly and strongly rejected the need to balance individual privacy interests against the interests of society in mental health treatment because private communications are essential for effective psychotherapy, and access to effective psychotherapy is in the best interest of both the individual and society. Jaffee v. Redmond, 116 S. Ct. 1923, 1932 (1996). This holding has been followed in more than 150 decisions in the past ten years.

**C. The Growing Threat to Health Information Privacy From Health Information Technology**

Congress has determined that the increasing use of information technology “has greatly magnified the harm to individual privacy that can occur”. Pub. L. 93-579, sec. 2(a)(2). HHS has determined that electronic information technology has “made it possible to breach the security and privacy of health information on a scale that was previously inconceivable.” 65 Fed. Reg. at 82,474. The absence of national privacy standards for health IT “has made the health care industry and the population in general uncomfortable about this primarily financially-driven expansion in the use of electronic data.” 65 Fed. Reg. at 82,466.

The President’s Information Technology Committee has determined that the nation’s interconnected electronic information systems are “highly vulnerable” to attacks, the number of attacks is growing by “over 20 percent annually” and the vulnerabilities cannot be adequately addressed without redesigning the IT systems “from the ground up”. “Cyber Security: A Crisis in Prioritization (Feb. 28, 2005).

Also, much has happened since the Senate last considered a “Wired for Health Care Quality Act” in 2005. HHS’ current Security Guidance instruction states that “these [electronic information] technologies have also created complications and increased the risk of loss and unauthorized use and disclosure of this sensitive information.”

The Government Accountability Office has found that

“While information technology can provide the means to protect the privacy of electronically stored and exchanged health information, the 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.”

“Health Information Technology: Early Efforts Initiated But Comprehensive Privacy Approach Needed for National Strategy”, GAO-07-238 (Jan. 10, 2007).

There have been repeated massive privacy breaches of electronic information systems. See “An Ominous Milestone: A 100 Million Data Leaks”, The New York Times (December 18, 2006); “Survey: 81% of U.S. Firms Lost Laptops With Sensitive Data In the Past Year”, Computer World (August 16, 2006). There have been unprecedented breaches of health privacy caused by electronic health information systems used by the government (“Vast Data Cache About Veterans Is Stolen”, The New York Times (May 23, 2006); “Veterans Administration Loses Data”, Consumer Affairs (February 18, 2007); “Medicare and Medicaid Gaps Are Found”, The New York Times (October 21, 2006)) and by the private health care sector (“Medical Data on Empire Blue Cross Members May Be Lost”, The New York Times (March 14, 2007), “ID Theft Infects Medicare Records”, The L. A. Times (September 25, 2006), “Patient Data Stolen—Nurse Loses Beaumont Laptop With 28,000 Names”, The Detroit News (August 23, 2006). The Government Accountability Office has concluded that government health insurance contractors as well as commercial health insurers often experience breaches of electronic information system that compromise the right to health information privacy. “Privacy: Domestic and Offshore Outsourcing of Personal Information in Medicare, Medicaid and TRICARE”, GAO-06-676 (Sept. 5, 2006).

When the Senate passed a similar bill in 2005 on the unanimous consent calendar, it could have claimed to have not been fully aware of the threat that health IT poses to the right to health information privacy. That is no longer possible, and the public is certainly aware of, and concerned by, the threat. Most Americans are “highly concerned” about the privacy of their health information. UPI Poll: Concern on Health Privacy” (Feb. 21, 2007); 62% to 70% of Americans are worried that their health information will be leaked from electronic information systems, Testimony of the Markel Foundation before the Senate Committee on Homeland Security and Governmental Affairs (Feb. 1, 2007); 66% of Americans believe Congress should make protecting electronic information systems a higher priority, Federal Computer Week (May 23, 2006), and 42% of Americans feel that “privacy risks outweigh expected benefits” from health IT. Harris/Westin Poll on EHR and Privacy (2006). It is time for Congress to acknowledge and respond to the growing concerns of the public.

Accordingly, we urge the Senate HELP Committee to hold hearings on the importance of preserving the patient's right to health information privacy in any electronic health information legislation.

## **II. Two Critical Questions: Privacy Essential for Quality and Cost Savings**

As Senators consider health IT legislation, they should also consider two critical questions:

- (1) Do they believe that health care patients have a right to health information privacy?
- (2) If so, do they believe that the patient's right to health information privacy should be recognized and protected in health IT legislation?

If the answer to either of these questions is "no", then access to quality health care, and specifically to effective psychotherapy, cannot be preserved, and an electronic health information system that the public will accept, is probably not possible.

HHS made an important fundamental finding in issuing the Original HIPAA Privacy Rule:

"In short, 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."

65 Fed. Reg. at 82,467. If individuals cannot trust that the most intimate details of their lives will be disclosed in routine situations only as they wish, those disclosures will not be made to anyone. Quality measures, evidence based medicine, an electronic health information system, and even a high quality health care system are not possible without strong privacy protections. Experience shows that we can have high quality health care without health IT, but we cannot have high quality health care without privacy. Thus, privacy standards are "consistent with the objective of reducing the administrative costs of providing and paying for health care". 65 Fed. Reg. at 82,474.

In fact, failure to build strong privacy measures into health IT legislation is likely to drive up the costs associated with medical disorders. According to HHS estimates, more than 2 million Americans each year delay or avoid treatment for mental illness due to privacy fears. 65 Fed. Reg. at 82,779. Thus, providing privacy protections that citizens want and expect would result in net economic

savings “from approximately \$497 million to \$795 million annually”, according to HHS findings. Id.

HHS has also estimated that 586,000 Americans did not seek earlier cancer treatment due to privacy concerns and that this delay has resulted in \$1.6 billion in lost wages. 65 Fed. Reg. at 82,777. HHS also has found similar privacy concerns delay the treatment of HIV/AIDS and other sexually transmitted diseases which leads to death, expensive fertility problems, fetal blindness, ectopic pregnancies and other reproductive complications. 65 Fed. Reg. at 82,778. Of course, the cost in increased human suffering from delayed or avoided medical treatment is incalculable.

Further, the Supreme Court has found, based on the “reason and experience” of the nation, that effective psychotherapy is completely dependent upon the patient’s justifiable expectation that communications with a psychotherapist will not be disclosed without the patient’s permission and that “the mere possibility of disclosure” may impede access to effective psychotherapy. Jaffee v. Redmond, 116 S. Ct. 1923, 1928 (1996). So failure to recognize and protect the patient’s right to health information privacy for mental health information will reduce or eliminate access to effective psychotherapy and increase costs associated with untreated mental illness.

### **III. The Draft Does Not Recognize or Protect the Patient’s Right to Health Information Privacy**

The draft bill repeatedly refers to “privacy and security” of health information but does not define those terms. See pp. 5, 11, 12, 19, 21, 26, 45, 63. Without such a definition, patients cannot determine what rights are being ensured and protected, and those who handle health information cannot be sure of their duties with respect to that information. As the National Committee on Vital and Health Statistics has noted, the imprecise use of privacy, confidentiality and security “often clouds discussions regarding privacy”. NCVHS letter to Secretary Leavitt, p. 2 (June 22, 2006).

#### **Recommendation #1**

We recommend that the following definitions be added to section 3001, the “Definitions; Reference section of the draft at p. 1:

“Health information privacy.—The term privacy means an individual’s right to control the acquisition, uses, or disclosures of his or her identifiable health data.

Confidentiality.—The term confidentiality refers to the obligations of those who receive information to respect the privacy interests of those to whom the data relate.

Security.—The term security refers to physical, technological, or administrative safeguards or tools used to protect identifiable health data.”

These definitions were adopted from the Institute of Medicine and are based on 18 months of hearings and deliberations by the NCVHS. NCVHS letter to Secretary Leavitt, p. 1.

### **Recommendation #2**

We recommend that the definition of “qualified health information technology” be modified to state that such technology must

- A. recognize that individuals have a right to health information privacy;
- B. provide individuals the opportunity to exercise their right to privacy by giving or withholding consent for the disclosure of identifiable health information, unless otherwise required by law;
- C. provide individuals the right to limit disclosure of certain health information to only designated practitioners (for example, patients should have the choice of allowing their mental health treatment information to be disclosed only to their treating psychiatrist);
- D. comply with all privileges (including the psychotherapist-patient privilege) and comply with all federal and state privacy laws, and
- E. not compel or coerce any practitioner to violate established standards of practice in his or her codes of professional ethics.

### **IV. The Draft Ensures That the Patient’s Interest in Privacy Will Generally Be Outweighed**

The draft bill provides that the Partnership and the Community will serve as a forum for “a broad range of stakeholders”. pp. 10, 17. However, the interests of individual stakeholders appear to be accorded equal weight, and consumers are in the minority in both committees, particularly relative to insurance plans and other third party payers, information technology vendors, and purchasers or employers. pp. 11, 19. However, no group has more “at stake” with respect to health information than the consumer. The consumer’s “stake” includes job opportunities, family relationships, and even his or her very health and life.

In addition, each committee is to include a representative from organizations “with expertise in privacy”, however, that expertise could quite literally be in eliminating privacy.

### **Recommendation #3**

At least 50% of the memberships in the Partnership and the Community should consist of consumer representatives, and no recommendation should be made by either committee that does not have the support of a majority of the consumer representatives.

The committees should also be required to include individuals from organizations with expertise in protecting the right to health information privacy.

### **Recommendation #4**

The Secretary of HHS should not adopt standards, particularly those that actually or potentially adversely affect the patient’s right to privacy without providing an opportunity for public comment in a rulemaking proceeding under 5 U.S.C. §553. See pp. 14, 15, 18.

### **Recommendation #5**

The Secretary’s discretion to adopt standards should be limited to adopting standards that are consistent with and preserve the patients’ right to health information privacy as reflected in Constitutional common law, the psychotherapist-patient privilege and the physician-patient privilege, and standards of professional ethics. pp. 15 and 18. The bill requires the Community to ensure an opportunity for participation with “outside advisors” with expertise in various areas, including “ethics”. Page 21. However, there is no requirement or incentive for the Community or the Partnership to recommend standards that are ethics-based or even consistent with standards of professional ethics.

### **Recommendation #6**

The Community and the Partnership should be required to identify and base recommendations to the Secretary on common elements of the right to health information privacy in Constitutional common law, standards of professional ethics, and state and federal law. pp. 13 and 16. The desire to implement a nationwide electronic health information system should be no justification for eliminating the basic elements of the constitutional, ethical, statutory and common law right to health information privacy.

**V. The Draft Does Not Ensure that Individuals will be Notified When Their Personal Health Information Is Wrongfully Disclosed**

The draft bill provides that patients are to be notified if their individually identifiable health information is “wrongfully disclosed”. pp. 17, 29, 43. However, GAO is to submit a report to Congress, not later than 12 months after the date of enactment, concerning the “necessity and workability” of requiring health plans, health care clearinghouses and providers to notify patients if their individually identifiable health information is wrongfully disclosed. p. 66.

At least 33 states now require notification of individuals when the privacy of their personal information is, or may have been, violated by breach of an electronic information system. Timely notification of security breaches of electronic health information systems is one of the “basic principles” adopted in a joint statement of the American Medical Informatics Association (AMIA) and the American Health Information Management Association (AHIMA). (September 7, 2006). Accordingly, there can no longer be any doubt that notification of the patient when their personal health information has been wrongfully disclosed is both “necessary and workable”. Of course, patients cannot exercise their right to health information privacy under state or federal law if they are not informed when their health privacy is violated.

**Recommendation #7**

Section 401 calling for a GAO report on the “necessity and workability” of notifying patients when their personal health information has been wrongfully disclosed should be deleted.

In addition, “wrongful disclosure” of a patient’s health information should include any disclosure that violates the patient’s right to health information privacy.

**The Wired for Health Care Quality Act Promotes the Use of “Nonidentifiable” Health Information But Does Not Define the Term**

The draft directs the Secretary to take actions to allow access to useful categories of “nonidentifiable health information”, but fails to define that term. Page 26.

**Recommendation #8**

Nonidentifiable health information should have the same meaning as “de-identified” health information under the HIPAA Privacy Rule. 45 C.F.R. §164.514(b).

## **VI. Expansion and Incorporation of the HIPAA Statute and Privacy Rule Reduce Rather Than “Ensure” Privacy**

The Wired for Health Care Quality Act references and expands HIPAA under the heading “Ensuring Privacy and Security”. Page 63. The HIPAA statute does not “ensure” privacy since it merely directs the Secretary to issue regulations setting forth “[t]he rights that an individual who is the subject of individually identifiable health information should have”. See §264(b)(1).

The Original HIPAA Privacy Rule tacitly acknowledged that patients had a right to health information privacy by recognizing the patient’s right of consent for the use and disclosure of identifiable health information for routine purposes. 45 C.F.R. §164.506 (65 Fed. Reg. at 82,810 (Dec. 28, 2000)). However, HHS under a different administration, eliminated the patient’s right of consent in routine situations in August of 2002. 67 Fed. Reg. at 53,212.

The HIPAA Privacy Rule currently in effect does not contain a right to health information privacy or consent for the routine use and disclosure of one’s identifiable health information. The Rule lists the patient’s rights under the Rule that must be included in a notice of privacy practices. Those rights are (a) the right to request restrictions (a consent process), (b) the right to receive confidential communications, (c) the right to inspect and copy protected health information, (d) the right to receive an accounting of disclosures of protected health information (other than for routine disclosures) and (e) the right to obtain a paper copy of the notice of privacy practices. The right to health information privacy is not listed among the patient’s rights. The right to request restrictions (a consent process) is rendered meaningless since covered entities can refuse the request for any reason or no reason. 45 C.F.R. §164.522(a)(1)(ii).

So the HIPAA Privacy Rule, as amended, makes no pretense of “ensuring” health information privacy. In fact, it provides that covered entities and their “business associates” may routinely use and disclose the individual’s identifiable health information (a) without notice of the use or disclosure or the information being disclosed, (b) without the patient’s consent or permission, and (c) even over the patient’s objection. 45 C.F.R. §§164.506, 164.522(A)(1)(ii).

In fact, HHS did not contest, and a Court of Appeals affirmatively held, that “covered entities” are, in fact, using the HIPAA Privacy Rule to violate the health information privacy of individuals against their will. Citizens for Health v. Leavitt, 428 F.3d 167, 176 (3<sup>rd</sup> Cir. 2006), cert. den. 127 S. Ct. 43 (2006).

So the draft Wired for Health Care Quality Act does not “ensure” health information privacy by relying on HIPAA. To the contrary, it diminishes the right to privacy by adding an additional “covered entity” (an operator of a health information data base) that may routinely use and disclose a patient’s identifiable health information without consent and over his or her objection. Page 63.

The National Committee on Vital and Health Statistics, the committee established by HIPAA to advise the Secretary on health information systems, has informed the Secretary that the HIPAA Privacy Rule is completely inadequate to address the needs of a national electronic health information system. NCVHS letter to Secretary Leavitt, pp. 9-10, 12-13. So it is plainly inadequate to rely on HIPAA for “ensuring privacy and security”.

### **Recommendation #9**

All references to the HIPAA statute and privacy regulations as “ensuring privacy and security” should be deleted, and privacy standards should be adopted that apply regardless of who handles the electronic health information.

## **VII. None of the Recommendations Above Are Inconsistent with HIPAA**

None of the recommendations listed above are inconsistent with HIPAA or the HIPAA Privacy Rule. When HHS amended the HIPAA Privacy Rule to eliminate the right of consent, it responded to overwhelming opposition from practitioners and consumers by stating that the privacy standards in the Rule were merely a “floor” of protections and were never intended to be a “best practices” standard or to supplant more stringent state laws or standards of professional ethics. 67 Fed. Reg. at 53,212. HHS also explained that practitioners could still provide a consent process at their option, if it was required by state law or if it was required by standards of professional ethics. 76 Fed. Reg. at 53,213.

So the recommendations for recognition and protection of the patient’s right to health information privacy are not inconsistent with, but merely build on to the “floor” of privacy protections contained in the HIPAA Privacy Rule. The fact that the recommendations add protections that the HIPAA Privacy Rule does not provide, does not “reopen HIPAA” any more than the provisions in the draft bill that provide for an “audit record” of all disclosures (p.5) or notice to the patient when health information is “wrongfully disclosed” (pp. 17, 29, and 43). The HIPAA Privacy Rule does not require an audit record of disclosures for routine purposes (45 C.F.R. §164.528(a)) nor does it require notice of privacy breaches. 45 C.F.R. §164.530(f).

## **VIII. Conclusion**

It can not longer be disputed that electronic information systems are a growing threat to health information privacy that is essential for quality health care. By grounding a nationwide health information system in traditional privacy principles, it should be possible for such a system to enhance rather than erode

the right to privacy. For this to happen, health IT legislation must contain basic privacy principles and provide an incentive for organizations to honor the patient's right to privacy. Health information technology and health information privacy are not incompatible.

"Reason and experience" teach, as the Supreme Court noted in the 1996 decision in Jaffee v. Redmond, that failing to protect the privacy of sensitive health information leads to less, rather than more, information. So the goals of an electronic health information system will likely be frustrated if the right to privacy that the public wants and expects is not protected. If citizens do not have a right to privacy for information such as genetic information or information revealing their inner-most thoughts and emotions, it is difficult to imagine a right to privacy for any information.

In a time of difficult decisions on how to finance needed health care, it is tempting to regard health IT as a source of savings. However, even the authors of the oft cited RAND study on health IT note that implementing such a system will cost \$280 billion over ten years and \$16 billion a year to maintain thereafter. "Can Electronic Medical Record Systems Transform Health Care? Potential Health Care Benefits, Savings, and Costs", Health Affairs, 1114 (Sept./Oct. 2005). Significant savings would not be achieved until the system is 90% implemented and used 100% of the time where it is implemented. This degree of implementation is likely to take eight years to achieve. "Savings in Electronic Medical Record Systems? Do It For the Quality", Health Affairs, 1124 (Sept./Oct. 2005). Some have observed that the RAND projections are based on "unproven assumptions", "wishful thinking" and "special effects". "Hope and Hype: Predicting The Impact of Electronic Medical Records", Health Affairs, 1121 (Sept./Oct. 2005). Of course, CBO scored a more modest version of the Wired for Health Care Quality bill as costing \$40 million in one year and \$652 million over 5 years.

Whatever the costs or savings, Congress should resist the temptation to sell the patient's right to privacy for the unproven and possibly illusory promise of health care savings. A health care system without privacy is not a health care system that the public wants.

As Congress and HHS have each found, privacy is a "fundamental right" that is one of the core values on which our system of government is based. Pub. L. 93-579, sec. 2(a)(4). 65 Fed. Reg. at 82,464. We are gravely concerned that this fundamental and essential right will cease to exist unless it is recognized and preserved in any health IT legislation.

We look forward to working with you to pass health IT legislation that contains the privacy rights that the public wants and expects and that we believe is essential to preserving access to effective psychotherapy.

Jim Pyles  
Counsel  
American Psychoanalytic Association  
Powers, Pyles, Sutter and Verville, P.C.  
Washington, D. C. 20005  
(202) 466-6550  
jim.pyles@ppsv.com