

**Protection of the Right to Health Information Privacy:
A Prerequisite for Health IT**

- I. **Any health IT system must**
 - A. **Recognize the patient’s right to health information privacy;**
 - B. **Provide an opportunity for that right to be exercised through informed consent;**
 - C. **Provide notice to the patient of actual or suspected breaches of health information privacy; and**
 - D. **Provide access to an effective remedy for breaches.**

- II. **Two practical reasons**
 - A. **“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. HHS Finding, 65 Fed. Reg. at 82,467 (Dec. 28, 2000).**

 - B. **Failure to protect the right to health information privacy leads to less, rather than more, health information because communications between practitioners and patients “would surely be chilled”. Supreme Court finding, Jaffee v. Redmond, 116 S. Ct. 1923, 1929 (1996).**

- III. **What is the right to health information privacy?**
 - A. **Health information privacy is an individual’s right to control the acquisition, uses, or disclosures of his or her identifiable health data.**

 - B. **Confidentiality is the obligations of those who receive information to respect the privacy interests of those to whom the data relate.**

C. Security is the physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure. Report of the National Committee on Vital and Health Statistics to Secretary Leavitt (June 22, 2006).

IV. What are the sources of the right to health information privacy?

A. “Privacy and confidentiality [of health information] are neither new concepts, nor 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.” Report to HHS, NCVHS (June 22, 2006).

B. Federal courts have found consistently that the right to informational privacy, as distinct from the right to decisional privacy, is protected by the Fourteenth, Fifth and Fourth Amendments to the United States Constitution. Whalen v. Roe, 97 S. Ct. 869, 877 (1977); Ferguson v. City of Charleston, 121 S. Ct. 1281, 1288 (2001), (“The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent.”); U.S. v. Scott, 424 F.3d 888 (9th Cir. 2005); Douglas v. Dodds, 419 F.3d 1097 (10th Cir. 2005).

C. In fact, the constitutionally protected right to privacy of highly personal information is so well established that no reasonable person could be unaware of it. Sterling v. Borough of Minersville, 232 F.3d 190, 198 (3rd Cir. 2000).

D. Ten states have a right to privacy expressly recognized in their state constitutions.

- E. A physician-patient privilege is recognized in the laws of 43 states and the District of Columbia. The State of Health Privacy, Health Privacy Project (2000).**
 - F. A psychotherapist-patient privilege is recognized in the laws of all 50 states and the District of Columbia. Jaffee v. Redmond, 116 S. Ct. 1923, 1929 (1996).**
 - G. All 50 states and the District of Columbia recognize in tort law a common law or statutory right to privacy of personal information. HHS finding 65 Fed. Reg. at 82,464.**
 - H. The right to not have health information disclosed without consent is reflected in the Hippocratic Oath dating from the 5th Century B. C. which is taken by most medical school graduates and in the standards of professional ethics adopted by virtually every segment of the medical profession. 65 Fed. Reg. at 82,472; The Use of the Hippocratic Oath: A Review of 20th Century Practice and a Content Analysis of Oaths Administered in Medical Schools in the U.S. and Canada in 1993, R. Orr, M. D. and N. Pang, M. D.**
- V. How do most Americans feel about health IT and privacy?**
- A. Most Americans are “highly concerned” about the privacy of their health information. UPI Poll: Concern on Health Privacy (February 21, 2007).**
 - B. 62% to 70% of Americans are worried that sensitive health information might leak because of weak data security; that there could be more sharing of patients’ health information without their knowledge; that computerization could increase rather than decrease medical errors; that some people won’t disclose necessary information to healthcare providers because of worries that it will be stored in computerized records; and that existing federal health privacy rules will be reduced in the name of efficiency. Testimony of the Markle Foundation before the Senate**

Committee on Homeland Security and Governmental Affairs (February 1, 2007).

- C. 66% of Americans believe Congress should make protecting information systems and networks a higher priority.**
 - 1. Of that group, 46% said they would have “serious” or “very serious” doubts about political candidates who do not support quick action to improve current laws. Federal Computer Week (May 23, 2006).**
- D. 42% of Americans feel that “privacy risks outweigh expected benefits” from health IT. Harris/Westin poll on EHR and Privacy (2006).**

VI. Health IT poses a threat to the right to health information privacy.

A. Congressional findings:

- 1. “Congress finds that...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;...the right to privacy is a personal and fundamental right protected by the Constitution of the United States...”. Pub. L. 93-579, section 2(a)(2) and (4).**

B. Presidential findings:

- 1. The nation’s interconnected electronic information systems are “highly vulnerable” to attacks,**

2. The number of attacks is growing by “over 20 percent annually”, and
3. The vulnerabilities can only be addressed by “fundamental research” to design security into IT systems “from the ground up.” “Cyber Security: A Crisis in Prioritization”, President’s Information Technology Advisory Committee, 5-12 (February 28, 2005).

C. HHS findings:

1. “The electronic information revolution is transforming the recording of health information so that 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.

D. Findings of the National Committee on Vital and Health Statistics (NCVHS):

1. “An EHR system creates greater risks to confidentiality because the comprehensive disclosures might include much more information than is necessary to the particular decision at hand.” NCVHS report to HHS (June 22, 2006).

E. Numerous articles in major publications over the past two years have detailed the privacy and other problems with electronic information systems.

1. “Data Theft Believed To Be Biggest Hack”, The New York Times (March 30, 2007).
2. “Medical Data on Empire Blue Cross Members May Be Lost”, The New York Times (March 14, 2007).

3. **“Warnings Over Privacy of U.S. Health Network”, The New York Times (February 18, 2007).**
4. **“Veterans Administration Loses Data”, Consumer Affairs (February 13, 2007).**
5. **“Have You Resold Your Data to Crooks?” Computer World (February 16, 2007).**
6. **“Kaiser Has Aches, Pains Going Digital. Patients’ Welfare at Stake in the Electronic Effort, Experts Say”, L. A. Times (February 15, 2007).**
7. **“Second Hospital Reports Lost Data. St. Mary’s Notifies 130,000 Days After Hopkins’ Notice”, The Baltimore Sun (February 13, 2007).**
8. **“Lost Computer Tapes Had Details of 135,000 Workers, Patients”, The Washington Post (February 8, 2007).**
9. **“GAO Report Confirms IT’s Threat to Privacy”, Modern Healthcare (February 6, 2007).**
10. **“Diagnosis Identity Theft: For \$60, a Thief Can Buy Your Health Records—and Use Them to Get Costly Care. Guess Who Gets the Bill”, Business Week (January 8, 2007).**
11. **“Spread of Records Stirs Patient Fears of Privacy Erosion”, The New York Times (December 26, 2006).**
12. **“LINK BY LINK; An Ominous Milestone: 100 Million Data Leaks”, The New York Times (December 18, 2006).**
13. **“Major Breach of UCLA’s Computer Files”, L. A. Times (December 12, 2006).**

14. **“Health Providers’ Social Security Numbers Posted on State Site”, Associated Press (December 8, 2006).**
15. **“Health Hazard: Computers Spilling Your History”, The New York Times (December 3, 2006).**
16. **“Setting the Records Straight—When You Sign Medical-Privacy Forms, What Exactly Are You Agreeing To? Probably Not What You Think.” The Wall Street Journal (October 21, 2006).**
17. **“Medicare and Medicaid Gaps Are Found”, The New York Times (October 8, 2006).**
18. **“ID Theft Infects Medical Records”, L. A. Times (September 25, 2006).**
19. **“Patient Data Stolen—Nurse Loses Beaumont Laptop With 28,000 Names, The Detroit News (August 23, 2006).**
20. **“Survey: 81% of U.S. Firms Lost Laptops With Sensitive Data In the Past Year”, Computerworld (August 16, 2006).**
21. **“Vast Data Cache About Veterans Is Stolen”, The New York Times (May 23, 2006).**
22. **“Hacker Steals Air Force Officers’ Personal Information”, The Washington Post (August 23, 2005).**
23. **“Regulators Fine Kaiser Unit \$200,000—The State Imposes the Penalty For Breaching Patient Confidentiality in Exposing Health Records on the Web.” The L. A. Times (June 21, 2005).**

**24. “Searches Conducted in Hacking Probe—
LexisNexis Estimates Breach Affects 310,000
People”, CNN.com (May 26, 2005).**

**25. “Personal Data for the Taking”, The New York
Times (May 18, 2005).**

**VII. How well has the federal government protected the patients’
right to health information privacy?**

**A. HHS “replaced” the patients’ right of consent in the
Original HIPAA Privacy Rule with “regulatory permission”
for covered entities and their business associates to
routinely use and disclose virtually any health information
without the patient’s permission and over the patient’s
objection. (August 14, 2002).**

**B. “Co-chair of HHS Advisory Panel Quits, Says Inadequate
Progress on Privacy Protections”, BNA Health Care Daily
(February 26, 2007).**

**C. “Loss of Personal Data at Federal Agencies Is
Widespread”, The Washington Post (October 16, 2006).**

**D. “To Agency Insiders, Cyber Thefts And Slow Response Are
No Surprise”, The Washington Post (July 18, 2006).**

**E. “Medical Privacy Law Nets No Fines—Lax Enforcement
Puts Patient Files At Risk, Critics Say”, The Washington
Post (June 5, 2006).**

**F. HHS Receives an “F” on its Computer Security Report
Card for 2005 and 2004 from the House Government
Reform Committee (March 16, 2006).**

**G. GAO has repeatedly found HHS fails to adequately protect
the patient’s right to health privacy.**

1. “Health Information Technology: Early Efforts

Initiated but Comprehensive Privacy Approach Needed for National Strategy”, GAO-07-238 (January 10, 2007).

- 2. “Privacy: Domestic Offshore Outsourcing of Personal Information in Medicare, Medicaid, and TRICARE”, GAO-06-676 (September 5, 2006).**
- 3. “Information Security: The Centers for Medicare & Medicaid Services Needs to Improve Controls Over Key Communication Network”, GAO-06-750 (August 30, 2006).**
- 4. “Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data”, GAO-06-674 (June 26, 2006).**
- 5. “Information Security: Department of Health and Human Services Needs to Fully Implement Its Program, GAO-06-267 (February 24, 2006).**
- 6. “Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems, GAO-05-231 (May 13, 2005).**

**James C. Pyles
On behalf of the American Psychoanalytic Association
Powers, Pyles, Sutter & Verville, P.C.
1501 M Street, 7th Floor
Washington, D. C. 20005
(202) 466-6550
jim.pyles@ppsv.com**

April 17, 2007