

**Testimony of Dr. Alan F. Westin, Professor of Public Law & Government Emeritus, Columbia University, and Director of the Program on Information Technology, Health Records, and Privacy**

**At the Hearing on Privacy and Health Information Technology, NCVHS Subcommittee on Privacy, Washington, D.C., Feb. 23, 2005**

---

**INTRODUCTION**

Good morning. My name is Alan Westin. I am Professor of Public Law & Government Emeritus, Columbia University, and Director of the Program on Information Technology, Health Records, and Privacy, a new activity of the non-profit Center for Social and Legal Research, which I head. I will describe the new program later in my testimony.

Issues of health care, technology, and privacy have been one focus of my research, writing, and advocacy for over forty years. A summary of my work in this area appears as Appendix One in this document.

I was asked to appear today to discuss current public attitudes toward health care and privacy, especially in the context of information technology applications and programs to develop a national Electronic Medical Record (EMR) system. I am very glad to see this topic of public attitudes included in the Advisory Committee's two days of discussions. I am convinced that how the public sees the privacy risks and responding actions in any EMR system will be absolutely critical to this program's success – or will be a major factor in its failure.

To address these issues, and to assist the Advisory Committee and HHS, my Program collaborated with Harris Interactive to place a set of exploratory questions on a representative national survey by telephone that Harris Interactive conducted this month, between February 8-13. The top line results and my analysis of their implications are being publicly released at this hearing, and will also be published in The Harris Poll.\* In about two weeks, our Program will publish a full survey report, with demographic and factor analyses that should be quite useful.

Our telephone survey had 1,012 respondents. The national sample was weighted to be demographically representative of the public 18 years of age or older. This represents approximately 214 million adults. The sampling error is plus or minus 3%. (The questionnaire we used and the top line results we obtained appear as Appendix Two to this testimony.)

-----  
Our Program and I are most appreciative of the contribution of David Krane of Harris Interactive to this survey and, as always, to the Harris Poll Chairman, Humphrey Taylor.

## **THE AMERICAN PUBLIC AND HEALTH-CARE PRIVACY: A BASELINE SUMMARY**

Our Program is aware of fourteen published national studies dealing in whole or in major parts with issues of health information privacy. We have summarized these in our Program's first publication – [How the Public Views Health Privacy: Survey Findings from 1978 to 2005](#). This is available free on the Program's web site, at [www.pandab.org](http://www.pandab.org)

Before describing our February 2005 survey results relating to the Electronic Medical Records program, it is helpful to lay in the core findings of past health privacy surveys. In summary:

- Surveys show consumers rate personal health information and financial information the two most sensitive types of consumer personal information
- Persons with chronic and especially genetically-based health conditions express sharp concerns about circulation and use of their health status to deny them important consumer opportunities and benefits
- Consumers also express concerns about privacy and security in the current move to greater collection and use of medical records electronically
- While 80% of online consumers go to health sites for information, they express high concerns about privacy and security in their surfing
- Because of their privacy concerns, many consumers using health information web sites do not share their personal data, and take full advantage of these sites
- Consumers also express fears that their health information might be accessed or used improperly to commit identity thefts

(Sources and details for these topline views are in the Program's paper referenced above.)

With these well-established majority public views as a starting point, we turn to our new February 2005 health privacy survey.

### **OUR 2005 SURVEY RESULTS**

#### **How the Public Sees Handling of Personal Health Information in the Health Care System Today**

We were able to use a trend question from 1993 to probe the public's views on this issue, so that we could have a pre- and post-HIPAA reading.

In the 1993 national survey on “Health Information Privacy” that Harris and I conducted, we asked respondents whether they believed that a list of health system participants had “disclosed your personal medical information in a way that you felt was improper?”

Over a fourth of the public – 27% – then representing 50 million adults, said they believed one or more of the listed persons or organizations had disclosed their personal medical information improperly. Specifically:

A doctor who has treated you or a family member.....	7%
A clinic or hospital that treated you or a family member .....	11
Your employer or a family member’s employer .....	9
A health insurance company .....	15
A public health agency .....	10

When we repeated this question in 2005, we asked about improperly-considered release by these same persons or organizations “in the past three years.” We recorded a dramatic drop in public perceptions of such improperly handled personal medical information.

In 2005, only 14% of the public – almost in half from 1993 – now believe their personal medical information has been released improperly. (While substantially lower than the 1993 results, it should be noted that this still represents 30 million adults in the current U.S. population).

The results in 2005 were down across each of the five categories, as follows:

A doctor who has treated you or a family member.....	5%
A clinic or hospital that treated you or a family member .....	8
Your employer or a family member’s employer .....	5
A health insurance company .....	8
A public health agency .....	5

This drop from 27% to 14% of the public may well represent effects with the public from the HIPAA Privacy Rule rollout since April 2003. We tested that in our next set of questions.

### **Experience With HIPAA Privacy Notices**

We informed respondents that “a Federal Health Privacy Regulation (called the HIPAA rule) has required all health care organizations to give patients a privacy notice explaining how the organization will collect and use the patient’s health information, how it will keep the information secure, how patients can get access to their own health records, correct any errors, and control most disclosures of their information to people outside the health care system.” We then asked: “Have you ever received one of these HIPAA health privacy notices?”

Given the ubiquity of HIPAA privacy notices – handed out by every doctor, dentist, clinic, hospital, pharmacy, health insurer, etc. – I had anticipated a yes response from well over 90% of respondents. I assumed that persons away studying in Tibet since April 2003 would be the kind of respondents who would say no.

I was wrong.

A third of the American public – 32%, representing 68 million adults – said they had never received a HIPAA privacy notice (and only 1% chose to say Not Sure). This is both a surprising and disturbing result, since it seems sure that most of these persons did have a Privacy Notice given to them since April 2003. Obviously, they do not recall the paperwork as the Privacy Notice we described.

Two-thirds of the public – 67% – recalled that they had received a HIPAA notice, representing 148 million adults.

### **Confidence in Medical Record Handling Post-HIPAA**

We followed up by asking respondents who remembered getting a HIPAA privacy notice personally – two thirds of the public – this question:

“Based on your experiences and what you may have heard, how much has this federal privacy regulation and the Privacy Notices affected your confidence that your personal medical information is being handled today in what you feel is the proper way?”

Two-thirds of the public (67%) said their confidence had been increased. Of these, however, only 23% said their confidence had been increased “a great deal,” while a much larger 44% chose “only somewhat.” Thirteen percent said “not very much” and 18% “not at all.”

### **EMR – Levels of Public Awareness**

With the questions just reported as a foundation, we moved on to probe public attitudes toward the EMR program. We first described what we called Electronic Medical Records – EMR:

“The Federal Government has called for medical and health care organizations to work with technology firms to create a nationwide system of patient Electronic Medical Records over the next few years. The goal is to improve the effectiveness of patient care, lessen medical errors, and reduce the costs of paper handling. Have you read or heard anything about this program?”

Our survey was conducted after President Bush had described the EMR program in his State of the Union message in January, and had also gone out to the Midwest in early February in several public meetings outlining and promoting EMR. However, since

this remains a rather specialized issue, not directly affecting consumers now, and not generating much public debate, I assumed knowledge would be low.

This time I was right.

Less than a third of the public – only 29% – said they had read or heard about a national EMR program. This represents 62 million adults, and a quick look at our demographic data showed that these were, predictably, primarily the better-educated, higher-income, technology-using members of the public.

### **EMR: Privacy and Security Concerns**

Having laid a foundation about EMR, we posed the following multi-part question to respondents:

“Here are some things that some people have said might happen under such a patient Electronic Medical Record system. How concerned are you [about each item read] – very concerned, somewhat concerned, not very concerned, or not concerned at all?”

The following list was used in a randomized order, with these results:

**Table One: The Public’s Privacy and Security Concerns in an EMR System**

<b>ITEM</b>	<b>Concerned (Very + Somewhat)</b>	<b>Very</b>
<b>Sensitive personal medical-record information might be leaked because of weak data security</b>	<b>70%</b>	<b>38%</b>
<b>There could be more sharing of your medical information without your knowledge</b>	<b>69</b>	<b>42</b>
<b>Strong enough data security will not be installed in the new computer system</b>	<b>69</b>	<b>34</b>
<b>Computerization could increase rather than decrease medical errors</b>	<b>65</b>	<b>29</b>
<b>Some people will not disclose sensitive but necessary information to doctors and other health care providers, because of worries that it will go into computerized records</b>	<b>65</b>	<b>29</b>
<b>The existing federal health privacy rules protecting patient information will be reduced in the name of efficiency</b>	<b>62</b>	<b>28</b>

Some observers of our survey may feel that respondents given a list of potential concerns in any program are likely to say that they share such feelings. This is not the record in most social-issue surveys and especially in privacy surveys over the past four decades.

In other consumer, citizen, and employee privacy surveys, including health privacy surveys, the public majority has demonstrated an ability to modulate its expressed concerns depending on its perceptions of the issues. In other words, when a list of potential privacy problems is offered to survey respondents, the American public majority can usually sort them out in a pretty sophisticated way – reflecting the public’s actual mood and perceptions on social issues, and not controlled by a general pro-privacy or anti-government or anti-business orientation.

This is proved in dozens of privacy surveys where concern levels expressed by respondents run the gamut from heavy to light to non-existent, depending on the public’s sense of the services offered, the privacy or anti-discrimination interests at stake, and how respondents believe a given program or process will be conducted.

Here, a solid two-thirds of the current American public – in a range from 62-70% – say they share the concerns of “some people” about adverse privacy and data security results taking place in the operations of an Electronic Medical Record system. And, those saying they are Very Concerned ranged from 28 to 42%.

These views are obviously shaped by general public awareness about the high incidence of identity thefts, a constant media “drip-drip” of stories about leakage or disclosure of personal consumer data from organizational databases, and accounts of hackers penetrating business and government web sites to steal personally identifying consumer files.

With these larger privacy-violation and data insecurity trends in the background, I believe our six-topic list represents the core of the privacy concerns that two-thirds of the public will be looking at – and want to have successfully addressed – before most Americans will be comfortable with an EMR system.

### **How the Public Divides on the Benefits and Privacy Risks of an EMR System**

It is commonplace in surveys of this kind, after describing a new program and then measuring various concerns about it, to pose a “tie-breaker” question. This asks, essentially, taking into account supposed benefits of some business or government program or action and also the risks to privacy or other social value you may see, where do you come out on the program’s acceptability to you?

Our tie-breaker question on EMR was framed as follows:

“Supporters of the new patient Electronic Medical Record system say that strong privacy and data security regulations will be applied. Critics worry that these will not be applied

or will not be sufficient. Overall, do you feel that the expected benefits to patients and society of this patient Electronic Medical Record system outweigh potential risks to privacy, or do you feel that the privacy risks outweigh the expected benefits?"

(The two alternatives were rotated in presentation to respondents to avoid presentation bias.)

And the winner was..... NO ONE.

The public divides equally on this fundamental question – 48% saying the benefits outweigh risks to privacy and 47% saying the privacy risks outweigh the expected benefits. The deciding 4% said they just weren't sure.

What I draw from this key question is that half the American public does not feel today that an EMR program is worth the risks to privacy that they perceive as accompanying this development.

**That is the reality that program advocates will need to consider, respond to, and overcome by a range of laws, rules, practices, technology arrangements, privacy promotions, and positive patient experiences – if EMRs are to win majority public support and high patient participation.**

### **Segmenting the Public on EMR Privacy Concerns**

In privacy surveys since 1991, I have created various segmentations of the public on consumer, citizen, and employee privacy issues. The goal is to ask sets of questions that tap basic orientations and preferences of respondents and, on most issues in a given area of privacy (health, financial, anti-terrorist powers, etc.) will identify High, Medium, and Low Privacy Concern segments of the public.

If the segmentation is sound, the total respondents will scale in their answers to the substantive policy issues involved in that area. The High respondents will express the sharpest privacy concerns, reject competing values, call for legal interventions, etc., while the Medium and Low respondents will each record less intense or little to no concerns. We can then look at the demographic characteristics of each segment, and gain some insights into the underlying bases of each position.

We created our EMR Privacy Concern Segmentation from responses to the six issues posed in the previous question discussed. Our units were:

**Concern chosen in 5 or 6 statements.....High EMR Privacy Concern..... 56%**  
**Concern chosen in 3 or 4 statements..... Medium EMR Privacy Concern .....16**  
**Concern chosen in 1 or 2 statements..... Low EMR Privacy Concern .....14**  
**Concern not chosen in any statement..... Not Concerned About EMR Privacy.....14**

The most obvious and important thing to note is that a solid majority of the American public today is in the High EMR Privacy Concern camp, representing a whopping 120

million adults. In comparison, only 35% of the public is in the High Privacy camp when it comes to overall consumer privacy issues.

Since we just received these survey data this past weekend, I am not able to present as yet the demographics on this segmentation, or on the populations represented in other questions. Our Program will prepare such a detailed report and issue it in approximately two weeks.

### **Empowering Patients From the Outset**

We considered it important to see how the public felt about the role that patients might play directly in any EMR system, not as passive subjects but as technologically-aided participants. Our question was:

“Since most adults now use computers, the new patient Electronic Medical Record system could arrange ways for consumers to track their own personal information in the new system and exercise the privacy rights they were promised. How important do you think it is that such individual consumer tools be incorporated in the new patient Electronic Medical Record system from the start?”

More than eight out of ten respondents – 82% – rated such consumer empowerment as important, and 45% of these considered it Very Important. Only 17% did not see this as important, with 1% not sure.

I view this result as a powerful, publicly-derived Privacy Design Specification for any national EMR system. It is a design approach that will be ignored, put off until a later time, or rejected as unworkable at the peril of any EMR system’s entire future.

### **CONCLUSIONS AND RECOMMENDATIONS**

I start my judgments with the belief that further computerization of health information and a national program to create an electronic medical records network is both inevitable and – potentially – a very good thing for patients, the health care system, and American society.

I also believe that such a program has far greater chances to be successful in this decade than ever before. We should remember that earlier health-information computerization programs – in the 1970s, 1980s, and 1990s – failed badly or made only marginal improvements in the health care system, at enormous outlays of money and effort. This was essentially, I believe, for two reasons: (1) because large majorities of health care practitioners were not ready – or able – to embrace the technology tools offered and (2) because of weaknesses in the software and system technologies at those points in time.

It is only now, when this generation of health care practitioners is comfortable with information technology – from their cell phones and laptops to their use of databases

and comfort in using medical and genetic research data – that greater computerization has the chance to succeed on the front lines of health service.

And it is only now that powerful new database and data mining technologies, along with data linkage techniques, may provide the bang for the buck that is needed to justify electronic medical records processes and networks.

Also, the EMR program is, fortunately, not one in which predominant business or government interests are in direct opposition to the main consumer and privacy advocacy communities, as is sometimes the case in privacy debates. Leaders in the health care community, health researchers, health data service providers, and government health programs have expressed concerns that strong privacy standards be installed, and are ready to help assure that patient privacy interests are protected – indeed advanced – in any EMR system. Of course, some privacy issues will divide the players in EMR debates, and finding ways to create privacy-enhancing solutions for those challenges will be critical.

Having said that, I return to the main theme from our new survey. If a national EMR program is to get anywhere with the American public – and through their views with the Congress and state legislators asked to appropriate the big bucks for EMR projects -- the half of the American public that believes the privacy risks outweigh the benefits will have to be persuaded.

This will not be done by the President or HHS executives just saying that, of course, the privacy of your personal information will be protected (although such assurances are very welcome).

What is required, I submit, is an active, well-funded, and impressively staffed program to bring Privacy By Design into the EMR program NOW. This should parallel the excellent ELSI (Ethical, Legal and Social Issues) Program that Congress funded as part of the Human Genome Project, jointly administered by NIH and the Department of Energy.

Such a Privacy by Design Working Group for EMR should apply the tested wisdom and methodologies of privacy analysis, privacy policy-making, and privacy policy implementation and oversight that emerged in the 1970s and has had many successes since. It must pursue five main tasks:

1. Conduct Continuing EMR Privacy Risk and Threat Assessments – to identify the predictable pressures on patient privacy both from within the health care setting and from the many industries and governmental functions that claim access to identified health information for their programs. While data security is involved – representing the way that organizations keep their promises of privacy and confidentiality – it is the privacy risks that this Design Group needs to focus on. And, this assessment is not a one-time, but continuous, function to be based

on case studies of operating EMR programs and reviews of each major new function being developed.

2. Design and Propose New Privacy Laws and Regulations to Accompany EMR Roll-Outs. The HIPAA Privacy Rules provide a good foundation but it will require laws and regulations tailored to the new EMR networks and systems.

3. Identify System Design Elements That Would Enhance Rather than Defeat Privacy Interests. A single integrated national patient record system, overseen by the federal government, no matter how benignly, would represent a privacy disaster. From the start, I believe, an EMR program should be designed to be decentralized but linked, with interoperable technologies, and with rigorous procedures for tracking personal information uses and movements in support of privacy rule observance.

4. Identify and test anonymization techniques to enable both advanced medical research and data-analysis services. From the start, EMR systems need to develop the identification filters and maskers that will enable researchers and data analysts to access anonymized health record sources. Surveys have shown the public to be very nervous about researcher access to their medical records, and this calls for powerful anonymizing processes to be installed, verified, and communicated to the public from the start, not retrofitted.

5. Identify and Test Procedures to Empower Individual Patients to Access the EMR Systems Directly, to Assert Their Privacy Rights and Carry Out Their Individual Privacy Choices. This will, inevitably, require techniques for secure identification of patients seeking direct access to the system, and probably a biometric ID. Properly administered, I view a patient and/or citizen biometric as inevitable by the end of this decade, since I cannot envisage empowering patients in the EMR systems without secure identification.

These activities might be initiated now, through a private non-profit association, and attached to the Regional EMR projects that have been organized. Both government and private funding should support such a Privacy by Design organization.

Finally, I believe that there needs to be an independent EMR Privacy Board, appointed soon, with a continuing problem-identification, investigative, and standards-recommending assignment. If privacy is just a subset of a larger EMR Standards Body, its proposals will almost surely be vetoed more than they will be minded.

Many more issues and activities of such an EMR Privacy By Design working group could be described. But my central point has been made. Without an active, well-funded and impressively-staffed EMR Privacy by Design function, privacy issues will be addressed too little and too late by EMR proponents – and at great risk to their important and promising idea.

## **OUR NEW PROGRAM ON INFORMATION TECHNOLOGY, HEALTH RECORDS, AND PRIVACY**

The survey I have reported here is one of the first activities of our new Program, officially created in January, 2005. It was formed by our Center for Social and Legal Research (which was itself created as a non-profit think tank in 1985 to explore technology-society relationships) because we see the re-shaping of the nation's health care system through advanced technology applications as one of the most important developments of the next two decades.

We outline this in a White Paper that will be available free in about two weeks at the Program's Home Page and library, which can be found at [www.pandab.org](http://www.pandab.org). The paper is titled Computers, Health Records, and Citizen Rights in the Twenty First Century, co-authored by myself and the Program's Associate Director, Vivian van Gelder.

Our Program plans to conduct six main activities, all centered on the privacy aspects of these explorations:

- Conduct Continuing Public Opinion Surveys of the public and various leadership groups, with Harris Interactive as our privacy partner.
- Conduct Empirical Case Studies of the privacy experiences in emerging health information technology experiments and programs.
- Develop Legal and Policy Analyses of the privacy, confidentiality, subject access, and due process aspects of a national or decentralized-model EMR system.
- Track the privacy rules and experiences in EMR projects of other democratic nations.
- Publish White Papers and Reports, and a Quarterly Electronic Newsletter
- Organize Seminars and Conferences on Program Themes

As already noted, we have opened a Home Page and library at [www.pandab.org](http://www.pandab.org). We invite everyone interested in following our work and receiving our products to register at the Program site – under its strong privacy policies, of course – and to share your thoughts and reactions with us.

Our staff and contact information are on the next page.

I would welcome questions and discussions from the Committee, and appreciate the opportunity to share our survey findings with this audience.

**Program on Information Technology, Health Records, and Privacy**  
**An Activity of the Center for Social and Legal Research**

---

**Director:**

Dr. Alan F. Westin, LLB, PhD  
Professor of Public Law & Government Emeritus, Columbia University

**Associate Director**

Vivian van Gelder, LLB

**Counsel**

Robert R. Belair, LLB

**Legal Staff**

John Haley, LLB  
Lyle Himmel, LLB  
Kevin Coy, LLB

**Program Administrator**

Lorrie Sherwood

**Communication Director**

Irene Oujo

**Research and Editorial**

Natalie Kochmar  
Christie Lawrence

**Administrative Assistant**

Julie Previzi

**Webmaster**

Hillary Sherwood

**Survey Organization**

Harris Interactive

**Contacts: Mail: Suite 414, Two University Plaza, Hackensack, N.J. 07601**

**Tel. (201) 996-1154      Fax (201) 996-1883      email: ctrslr@aol.com**

**Dr. Westin's direct email: alanrp@aol.com**

## Appendix One

### Dr. Alan F. Westin

#### Director, Program on Information Technology, Health Records and Privacy

Dr. Alan F. Westin is Professor of Public Law and Government Emeritus at Columbia University, where he taught for 37 years. He is the founder of the Center for Social & Legal Research and President of its *Privacy & American Business* activity. Dr. Westin is the author or editor of 26 books on constitutional law, civil liberties, American politics, and privacy, and has been listed in Who's Who in America for three decades.

Professor Westin's first major books on privacy – Privacy and Freedom, published in 1967, followed by Databanks in a Free Society 1972 (for the National Academy of Sciences)– are considered seminal works on privacy. Each correctly predicted how advances in data surveillance of the mid-1960s and new computer and telecommunication applications of the 70s would affect American organizations that keep records about consumers, employees, and citizens, from hospitals, health and life insurers, credit bureaus, banks to colleges, police, and welfare agencies. Both books called for creating new laws, new organizational policies, and continuous new-technology privacy assessments in the governmental, business, and non-profit areas, if basic privacy values and rights were to be preserved in an increasingly information-technology driven world.

Dr. Westin is a leading authority on consumer-privacy public opinion surveys, and in understanding and interpreting the privacy attitudes of the American consumer. He has worked with Louis Harris & Associates (now Harris Interactive) and Opinion Research Corporation on over 50 national surveys since 1978 exploring consumer privacy issues. He has created privacy indices, which are universally used and quoted. His reports on consumer privacy concerns and attitudes have been featured in the New York Times, Wall Street Journal, Consumer Reports, and dozens of other national publications, and he is a frequent commentator about consumer privacy on national television and radio.

Dr. Westin was the principal expert witness in the enactment of the first two national privacy laws in the United States – the Fair Credit Reporting Act of 1970, providing consumer rights in the credit-bureau industry, and the Federal Privacy Act of 1974. Over the past forty years, he has been a member of U.S. federal and state government privacy commissions; an expert witness before legislative committees and regulatory agencies; and a privacy consultant to many U.S. federal, state, and local government agencies, such as, at the federal level, the Census Bureau, Social Security Administration, General Services Agency, Department of Commerce, and Office of Technology Assessment.

Dr. Westin has also advised many consumer-product companies, including IBM, American Express, Citicorp, Bell Atlantic, Empire Blue Cross and Blue Shield, Equifax, Microsoft, Chrysler, and Prudential Insurance, on privacy governance and policies within their companies as they effect their consumer-business relationships.

### **Health Information Privacy Activities**

Since the mid-1960s, Professor Westin has maintained a continuing special interest in medical confidentiality and health-information-systems privacy issues.

A comprehensive field study of computerization trends and health information was led by Dr. Westin for the U.S. National Bureau of Standards between 1974-76, and produced Westin's report on Computers, Health Records, and Citizen Rights (1976). The Privacy Code this report recommended was sent by NBS to every hospital in the U.S., and served as a model for hundreds of hospital and health institutions. The NBS Report was the leading empirical study of how computer use in the late 1960's and early 1970's was affecting the three main zones of health information use – direct care, payment and quality-assurance, and social uses of medical data.

Between 1978 and the early 1980s, he served as Research Director of the National Commission on Confidentiality of Health Records, a national association composed of the major health-care provider, payer, and quality-care associations in the United States. During this period, he spoke frequently on privacy and health information issues at national conventions or special meetings of the American Medical Association, Health Insurance Association, American Medical Records Association, American Orthopsychiatric Association, American Psychiatric Association, and many other health-professional groups.

Dr. Westin has been a featured speaker at the U.S. Department of Health and Human Services Privacy Task Force Conference on Medical Records and Privacy (February 1993); a reviewer of reports on privacy for the National Institute of Medicine (on emerging regional health data systems), the Journal of the American Medical Association, and for the U.S. Office of Technology Assessment (on privacy and the computerized medical record).

Dr. Westin was the privacy advisor to an award-winning 1994 Public Television Special Documentary on "Privacy and Health in the American Workplace." Dr. Westin drafted a national corporate-employee and human resources executives survey conducted by Louis Harris and Associates for use on this program, covering employee health and privacy issues in depth.

In 1993, he served as the academic advisor for a national public and leaders Harris survey on "Health Information Privacy." Results from this survey were released at a national conference in Washington, D.C. in November 1993, at which Dr. Westin spoke, co-sponsored by the U.S. Office of Consumer Affairs, the American Health Information Management Association, and Equifax Inc.

Also in 1993-95, Dr. Westin served as Principal Investigator on a 15-month project on privacy issues in the uses of genetic testing and genetic-test applications, funded by the U.S. Department of Energy for the Human Genome Project and its ELSI Program (Ethical, Legal and Social Issues). In 1997-99, he led a study of future uses of genetic

testing in the Life Insurance Industry, commissioned from the Center for Social and Legal Research by State Farm Insurance Company.

Over the past three years, Dr. Westin has led discussions of the HIPAA Privacy Rules at many national conferences. He has been a privacy consultant to several major pharmaceutical companies, from Eli Lilly, Glaxo Welcome and Smith Kline to Merck. He was also privacy consultant to Empire Blue Cross, Blue Shield; State Farm Insurance; and Mutual of Omaha. Dr. Westin also led a Global HR Privacy Policy Development project of Privacy & American Business, covering trans-border personnel data flows of multi-national firms that involved the worldwide handling of medical and health data by those companies.

In January 2005, Dr. Westin created the Program on Information Technology, Health Records and Privacy. Its first activity is the release of a new survey in February 2005, "How the Public Sees Health Records and an Electronic Medical Record Program," for which Dr. Westin served as Academic Advisor.

Dr. Westin views the re-shaping of the nation's health care system through advanced technology applications as one of the most important technology-society developments of the next two decades. It will be a priority of the new Program to help insure that privacy interests and patient empowerment are embedded in any new Electronic Medical Record systems -- from the start.

+++++

## Appendix Two

HARRIS INTERACTIVE, INC.  
161 SIXTH AVENUE  
NEW YORK, NEW YORK 10013

February 16, 2005

### PROGRAM ON INFORMATION TECHNOLOGY, HEALTH RECORDS AND PRIVACY

#### CENTER FOR SOCIAL & LEGAL RESEARCH

#### *TOPLINE RESULTS DATASHEETED QUESTIONNAIRE*

Study No. 23283  
Field Period: February 8 – 13, 2005  
Sample: 1,012 adults aged 18 or over

#### **Methodology**

Harris Interactive conducted this survey by telephone within the United States between February 8 and 13, 2005 among a nationwide cross section of 1,012 adults (ages 18 and over). Figures for age, sex, race, education, number of adults, number of voice/telephone lines in the household, region and size of place were weighted where necessary to align them with their actual proportions in the population.

In theory, with a probability sample of this size, one can say with 95 percent certainty that the results for the total sample have a **sampling error precision of plus or minus 3 percentage points** of what they would be if the entire U.S. adult population had been polled with complete accuracy. Statistical precision for the smaller samples is plus or minus 5 percentage points. Unfortunately, there are several other possible sources of error in all polls or surveys that are probably more serious than theoretical calculations of sampling error. They include refusals to be interviewed (nonresponse), question wording and question order, interviewer bias, weighting by demographic control data and screening (e.g., for likely voters). It is impossible to quantify the errors that may result from these factors.

#### Notes on reading the results

The percentage of respondents has been included for each item. An asterisk (\*) signifies a value of less than one-half percent. A dash represents a value of zero. Percentages may not always add up to 100% because of computer rounding or the acceptance of multiple answers from respondents answering that question.

**SECTION 650: HEALTH PRIVACY QUESTIONS [WESTIN]**

**BASE: ALL RESPONDENTS**

**Q650** [1] In the past three years, do you believe that [Insert each item] has disclosed your personal medical information in a way that you felt was improper, or not?

[RANDOMIZE]

	1 Yes	2 No	8 Not Sure (v) %	9 Decline to answer (v) %
<b>Q651</b>				
1 A doctor who has treated you or a family member *	5	94	1	
2 A clinic or hospital that treated you or a family member *	8	91	1	
3 Your employer or a family member's employer *	5	94	1	
4 A health insurance company *	8	90	1	
5 A public health agency *	5	93	2	
NET		14%		

**BASE: ALL RESPONDENTS**

**Q655** [2] Since 2000, a Federal Health Privacy Regulation (called the HIPAA Rule) has required all health care organizations to give patients a privacy notice explaining how the organization will collect and use the patient's health information, how it will keep the information secure, how patients can get access to their own health records, correct any errors, and control most disclosures of their information to people outside the health care system. Have you ever received one of these HIPAA health privacy notices?

	%
1 Yes	67
2 No	32
8 Not sure (v)	1
9 Decline to answer (v)	-

**BASE: HAVE RECEIVED HIPAA PRIVACY NOTICES (Q655/1)**

**Q670** [3] Based on your experiences and what you may have heard, how much has this federal privacy regulation and the Privacy Notices affected your confidence that your personal medical information is being handled today in what you feel is a proper way? Has it increased your confidence...?

	%
1 A Great Deal	23
2 Somewhat	44
3 Not Very Much	13
4 Not At All	18
8 Not sure (v)	1
9 Decline to answer (v)	*

**BASE: ALL RESPONDENTS**

**Q675** [4] The Federal Government has called for medical and health-care organizations to work with technology firms to create a nationwide system of patient Electronic Medical Records over the next few years. The goal is to improve the effectiveness of patient care, lessen medical errors, and reduce the high costs of paper handling. Have you read or heard anything about this program?

	%
1 Yes	29
2 No	71
8 Not sure (v)	-
<u>9</u> Decline to answer (v)	-

**BASE: ALL RESPONDENTS**

**Q685** [6] Here are some things that some people have said might happen under such a patient Electronic Medical Record system. How concerned are you that (READ EACH ITEM) – very concerned, somewhat concerned, not very concerned, or not concerned at all?

<b>Q686</b> [RANDOMIZE]		1 Very Concerned %	2 Somewhat Concerned %	3 Not Very- Concerned %	4 Not Concerned at all %	8 Not Sure (v) %	9 Declin to Answer %
1	Computerization could increase rather than decrease medical errors 13    1    -	29	36	22			
2	Sensitive personal medical-record information might be leaked because of weak data security 13    1    -	38	32	16			
3	There could be more sharing of your medical information without your knowledge 13    *    -	42	27	18			
4	Some people will not disclose sensitive but necessary information doctors and other health care providers, because of worries that it will go into computerized records 13    1    -	29	36	20			
5	Strong enough data security will not be installed in the new computer system 12    1    *	34	35	18			
6	The existing federal health privacy rules protecting patient information will be reduced in the name of efficiency 14    1    *	28	34	23			

**Privacy Concerns Segmentation**

	%
High	56
Moderate	16
Low	14
Very Low	14

**BASE: ALL RESPONDENTS**

**Q690** [7] Supporters of the new patient Electronic Medical Record system say that strong privacy and data security regulations will be applied. Critics worry that these will not be applied or will not be sufficient. Overall, do you feel that the expected benefits TO PATIENTS AND SOCIETY of this patient Electronic Medical Record system outweigh potential risks to privacy, or do you feel that the privacy risks outweigh the expected benefits? [PROGRAMMER NOTE: ROTATE THE EXPECTED BENEFITS OUTWEIGH POTENTIAL RISKS AND PRIVACY RISKS OUTWEIGH EXPECTED BENEFITS]

1	Benefits outweigh risks to privacy	48
2	Privacy risks outweigh the expected benefits	47
8	Not sure (v)	4
9	Decline to answer (v)	1

**BASE: ALL RESPONDENTS**

**Q695** [8] Since most adults now use computers, the new patient Electronic Medical Record system could arrange ways for consumers to track their own personal information in the new system and exercise the

privacy rights they were promised. How important do you think it is that such individual consumer tools be incorporated in the new patient Electronic Medical Record System from the start? Is it...?

	%
1 Very Important	45
2 Somewhat Important	37
3 Not Very Important	11
4 Not Important at all	6
8 Not sure (v)	1
9 Decline to answer (v)	*