

## Public Attitudes Toward Electronic Health Records

By Dr. Alan F. Westin

In his State of the Union Address, and in later speeches throughout the Midwest, President Bush proposed a \$125 million commitment to a national electronic medical record system. The value, he said, is in bringing better care to patients, improving the healthcare system and bringing the industry into the 21<sup>st</sup> century. With \$50 million of government funds already invested, most experts believe that increased computerization and a potential national network of electronic health records (EHR) are highly likely.

So, what about privacy?

To address these issues, P&AB's IT, Health Records and Privacy Program (see page 9 for more information) collaborated with Harris Interactive to place a set of exploratory questions on a representative national survey by telephone that Harris Interactive conducted February 8-13. This survey, *How the Public Sees Health Records and an EHR System*, was publicly released at the February 23 HHS Hearings on Privacy and Health Information Technology.

### The American Public and Healthcare Privacy: A Baseline Summary

Before describing our February 2005 survey results focused on the Electronic Health 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.

Continued on page 3

### ISSUE AT A GLANCE

#### In Depth: Electronic Health Records and Privacy

- *Public Attitudes Toward EHR*
- *Privacy Recommendations for a National EHR System*
- *New P&AB IT, Health Records & Privacy Program* . . . . . 1

#### South Korea's Personal Information Dispute Mediation Committee

*Koreans adopt a new approach to privacy dispute resolutions.* . . . . . 10

#### Missed P&AB's Tele/Web Conference?

*You can still listen in.* . . . . . 12

#### Workplace Monitoring:

#### Overcoming the Us v. Them Hurdle

*What business can do to foster trust at the workplace.* . . . . . 13

- 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.

**30 million Americans believe their personal medical data has been improperly disclosed**

(Sources for these findings are available in the Program's publication, *How the Public Views Health Privacy: Survey Findings from 1978-2005* available at [www.pandab.org](http://www.pandab.org).)



*Dr. Alan Westin, P&AB's President and Publisher*

### How the Public Sees Handling of Personal Health Information in the Healthcare 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 Westin-Harris 1993 national survey, *Health Information Privacy*, we asked respondents whether they believed that a list of health system participants had disclosed their personal medical information in a way that they 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:

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%

(Source: Health Information Privacy, 1993)

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.

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%

(Source: How the Public Sees Health Records and an EMR System, 2005)

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 healthcare 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 healthcare 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 – say 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 Health 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.”

### EHR – Levels of Public Awareness

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

“The Federal Government has called for medical and healthcare organizations to work with technology firms to create a nationwide system of patient Electronic Health 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 EHR 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 EHR. However,

**Only 29% say they have read or heard about a national EHR program**

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 EHR 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.

### EHR: Privacy and Security Concerns

Having laid a foundation about EHR, 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 Health 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:

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

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.

**The views of those concerned about medical data leaks are shaped by general public awareness of identity theft**

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 Health 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 theft, 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 websites 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 EHR system.

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

It is common 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 EHR was framed as follows:

“Supporters of the new patient Electronic Health 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 Health Record system outweigh potential risks to privacy, or do you feel that the privacy risks outweigh the expected benefits?”

**Half the American public feels an EHR system isn't worth the privacy risks**

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 EHR 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 EHRs are to win majority public support and high patient participation.

## Segmenting the Public on EHR 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 EHR 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 EHR Privacy . . . . .	14%
Concern chosen in 3 or 4 statements . . . . .	Medium EHR Privacy Concern . . . . .	56%
Concern chosen in 1 or 2 statements . . . . .	Low EHR Privacy Concern . . . . .	16%
Concern not chosen in any statement . . . . .	Not Concerned About EHR Privacy Concern . . . . .	14%

“Since most adults now use computers, the new patient Electronic Health 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 Health 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 EHR 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 EHR system’s entire future.

**82% say consumer empowerment is important in an EHR system from the start**

The most obvious and important thing to note is that a solid majority of the American public today is in the High EHR 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.

**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 EHR system, not as passive subjects but as technologically-aided participants. Our question was:

*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 topline results, full testimony and the Program’s first publication, How the Public Views Health Privacy: Findings from 1978-2005, are all available at www.pandab.org. The full survey report and a White Paper will be posted at our website soon.*

**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 overall sample have a sampling error of plus or minus 3 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. ■



# Privacy Recommendations for a National EHR System

By Dr. Alan F. Westin

Further computerization of health information and a national program to create an electronic health records (EHR) network is both inevitable and – potentially – a very good thing for patients, the healthcare system, and American society.

## Greater Chances of Success

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 healthcare system, at enormous outlays of money and effort. This was essentially for two reasons:

- Because large majorities of healthcare practitioners were not ready – or able – to embrace the technology tools offered
- Because of weaknesses in the software and system technologies at those points in time.

It is only now, when this generation of healthcare practitioners is comfortable with information technology, that greater computerization has the chance to succeed on the front lines of health service. From their cell phones and laptops to their use of databases, healthcare practitioners are using computerized medical and genetic research data.

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 health records processes and networks.

## Patient Privacy Comes First For All

Also, the EHR 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 healthcare 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

**An EHR network is potentially a good thing for patients, the healthcare system and American society**

are protected – indeed advanced – in any EHR system. Of course, some privacy issues will divide the players in EHR debates, and finding ways to create privacy-enhancing solutions for those challenges will be critical.

## American Public Needs Persuading

Having said that, I return to the main theme from our new survey. If a national EHR 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 EHR 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).

## Privacy by Design

What is required, I submit, is an active, well-funded, and impressively staffed program to bring Privacy By Design into the EHR 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 EHR 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 EHR Privacy Risk and Threat Assessments** – to identify the predictable pressures on patient privacy both from within the healthcare 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

**What is required is Privacy By Design in the EHR program NOW**

to focus on. And, this assessment is not a one-time, but continuous, function to be based on case studies of operating EHR programs and reviews of each major new function being developed.

2. **Design and Propose New Privacy Laws and Regulations to Accompany EHR Roll-Outs.** The HIPAA Privacy Rules provide a good foundation but it will require laws and regulations tailored to the new EHR 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 EHR 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, EHR 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 EHR 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 EHR systems without secure identification.

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

### **EHR Privacy Board Should Be Appointed**

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

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

