

Why Opt-out for Comprehensive Electronic Medical Information is Not Good Public Policy

William A. Yasnoff, MD, PhD

In building a system that ensures the availability of comprehensive electronic patient records when and where needed, public trust is clearly a critical issue. Each patient must be fully confident that their information will be used only for their benefit, and not be available for unauthorized purposes. The public understands clearly that making medical records electronic provides tremendous opportunities for improvements in care, but also increases the potential for misuse. Therefore, stronger privacy protections are needed for a system of electronic records.

When people have their medical information automatically included in a system where they only have the opportunity to opt out, they essentially participate without affirmative consent. The message to people is "We need your information so that we can take good care of you -- it's for your own good." The natural response to such an assertion is, "If you need the information for my own good, why don't you just ask my permission (which I would give, since it's for my own good)? Since you're not asking my permission, I can only assume that you really want the information for your good -- not mine." Therefore, failing to seek consent interferes with trust, rather than promoting it.

In addition, at least two major problems can be anticipated with an opt-out approach. First, those consumers that wish to have any control over their information will in fact opt out. Two recent surveys found that between 13% and 17% of consumers already admit to "information hiding" behavior in healthcare -- such as obtaining treatment out of state to conceal it from their primary provider or getting a lab test under an assumed name (California Healthcare Foundation, 2005: <http://www.chcf.org/topics/view.cfm?itemID=115694> , Harris Interactive, 2007: <http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Health-Privacy-2007-03.pdf>). All those people will likely opt out of the system, as well as those who are engaged in similar activities but were not comfortable admitting such behavior in a survey.

It is also important to consider what might happen when about 15% of people are disgruntled with an information system that provides them with no control and no benefit. It is entirely possible that this group will organize politically, protest the system, and force it to be shut down in its entirety. Indeed, this is exactly what happened in 1996 upon passage of the Health Insurance Portability and Accountability Act (HIPAA), which included a unique patient identifier for all Americans. While it seemed like a reasonable public policy to Congress and the President, the public became extremely concerned about the potential privacy problems that might result. They wrote to their Congressional representatives and, within a very short period of time, that provision of HIPAA was effectively repealed. Clearly, nowhere near 15% of Americans were even aware of the unique identifier provision of HIPAA, much less took the initiative to complain. However once even a small, vocal minority becomes upset with such a provision in the law, it is unlikely to survive over the long term.

Therefore, in building an information system to make comprehensive electronic patient information available when and where needed, it is not really a choice to avoid patient consent, as opt-out attempts to do. Protecting privacy with a single, unitary policy, such as opt-out, will always result in strong opposition, regardless of the specific policy. The only privacy policy everyone can agree on is that each person is able to determine their own customized privacy policy.

One common objection to this approach is that it is administratively and technically burdensome and/or infeasible. This is incorrect. Administratively, we already seek and receive

consent from every patient for every treatment. Adding consent for the use of information in conjunction with that treatment is a very minimal additional burden (if any). From a technological standpoint, maintaining records of consent and applying those to the use of information is a capability that has already been implemented in a number of existing, available systems, including at least one that is open source. Therefore, these objections appear to be excuses to appropriate patient information without consent.

Another objection is that many patients will not consent. In places that have used opt-in, this has not been the case. Massachusetts, for example, reported in January, 2009, that 94% of patients agreed to opt-in when asked (<http://www.nehimss.org/smart05-bin/public/downloadlibrary?&itemid=70172444211127087675>).

Finally, an opt-out model cannot allow access to mental health, substance abuse, HIV and genetic testing (as this would violate both state and Federal law). An opt-in model can provide this information with patient consent.

The best way to ensure trust in electronic records is to give patients control over their information. This also provides the opportunity to warn and educate patients who may consider withholding some of their information by giving them appropriate messages when they are indicating their preferences. This reduces provider liability because any decision to withhold information by patients is clearly and irrefutably documented.

Patient control is a non-partisan policy issue, with support from both the conservative Heritage Foundation (Haislmeier E: Health Care Information Technology: Getting the Policy Right, 7/16/06, <http://www.heritage.org/Research/Reports/2006/06/Health-Care-Information-Technology-Getting-the-Policy-Right>) and the liberal Progressive Policy Institute (Trusted Third Parties for Personal Health Records & Patient Privacy Briefing, 12/15/06, http://www.ppionline.org/ppi_ci.cfm?contentid=254135&knlgAreaID=126&subsecid=900096 and Recommendation for Electronic Health Records and Patient Privacy Protection in the Stimulus Bill, 1/15/09, http://www.ppionline.org/ppi_ci.cfm?contentid=254881&knlgAreaID=111&subsecid=138).

"The overriding requirement for public trust [in a system that provides comprehensive electronic medical records] is to engage patients in the control of their own information. This provides a realistic and practical solution for privacy policy since each person can then establish whatever policy they wish and change it anytime they deem it necessary. It is wishful thinking to believe that it is possible to develop a set of "universal" privacy policies that everyone (or even most people) could endorse. Even if such a task were possible, the resultant policies are likely to be so complex and voluminous as to defy easy understanding. More importantly, allowing each person to control their own information greatly reduces the trust level needed for the organization actually holding the information. Without patient control, the organization must be trusted not only to hold and safeguard the sensitive medical information (which is necessary in any case), but also to make independent decisions about its release. Such independent decisions, presumably made according to established (but complex) policies, would be subject to endless interpretation and challenge. With patients in control, the data holder is responsible only to follow instructions from each individual about data access and release. The latter is equivalent to the responsibility of financial banks to follow account-holder instructions about disbursements." [Miller HD et al: Personal Health Records: The Essential Missing Element in 21st Century Healthcare (HIMSS, 2009), p. 100]