Points to Consider in Ethically Constructing Patient-Controlled Electronic Health Records

August 21, 2012

Eric M. Meslin, Sheri Alpert, Aaron E. Carroll, Jere D. Odell, Peter H. Schwartz

Indiana University Center for Bioethics

This publication was supported by Award No: 90HT0054/01, a cooperative agreement program from the US Department of Health and Human Services, Office of the National Coordinator for Health IT to Indiana Health Information Technology, Inc. (IHIT) under the State HIE – Challenge Grant Program to the Indiana University School of Medicine and Regenstrief Institute, Inc. Its contents are solely the responsibility of the authors and do not reflect the official views of the Office of the National Coordinator for Health IT.

410 W. Tenth Street Suite 3100 Indianapolis, IN 46202
(317) 278-4034 phone (317) 278-4050 fax www.bioethics.iu.edu

Points to Consider in Ethically Constructing Patient-Controlled Electronic Health Records

August 21, 2012

Indiana University Center for Bioethics

On February 29, 2012, the Indiana University Center for Bioethics convened a one-day workshop of nationally recognized experts* in philosophy and ethicists, health information technology and systems, and health policy and health law. The purpose of the workshop was to solicit comments, critiques, and suggested changes to the draft of the Points to Consider document and its underlying ethics framework. We are grateful to the workshop participants for their time, interest, and input. Their involvement, however, implies neither their responsibility for nor their endorsement of the contents, or for how we interpreted and/or applied their input.

INTRODUCTION

Patient advocates and leaders in informatics have long proposed that patients should have greater ability to control the information in their electronic health record (EHR), including how it can be accessed by their health care providers[a]. The value of such "granular" control[b], as it has been termed, has been supported prominently in an influential report by the President's Council of Advisors on Science and Technology (PCAST).(2) Recently, the U.S. Department of Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology (ONC) funded several projects to study key components of EHR systems, including exploring ways to allow granular control.(3)

The argument for patient granular control in clinical encounters[c] follows from developments over the past three decades aimed at supporting patient empowerment and

---

[a] Note that in this document "health care providers" refers to physicians nurse practitioners, and physician assistants who provide independent clinical care. While many others are involved in patient clinical care, the issues raised by considering their access to the EHR raises distinct issues that will need to be addressed at a later date.

[b] Granular control authorizes or excludes the exchange of specific pieces of information in the EHR.(1)

[c] This document examines granular control in the clinical context and does not explicitly consider the myriad additional issues that arise from secondary uses of EHRs (as defined by HIPAA as uses beyond treatment, payment, and health care operations). In particular we do not consider research uses. This and all other non-treatment uses warrant separate study and analysis.

informed choice in the clinical encounter. [4, 5] Indeed, the argument for patient control of EHR[d] information can be seen as a logical extension of arguments for patient autonomy in decision making about medical treatment and research generally.[6-10] The concept of granular control also addresses the fundamental interest that individuals have in informational privacy. This interest is generally exercised, at least in part, through the ability to limit access by others to personal information. It is for these reasons that the promotion of Fair Information Practices (FIPs) has become important in many areas.[11, 12] Providing these types of controls may be seen to re-balance the relationship between clinician and patient, to promote trust, and to enhance overall quality of care.[13]

At the same time, granular control over content, access, and use of the EHR in the clinical context differs from other areas where respect for autonomy has been stressed, such as participation in a research study, where patients can exercise choice by declining to participate or withdrawing once enrolled. Nor is granular control of the EHR equivalent to acceptance of a recommended medical treatment, where patients have the right to a second opinion. In the case of EHRs, exercising unbridled control could have significant unintended negative consequences for patients and perhaps their families. For example, an individual might decide to keep his cardiologist from being able to see information regarding psychiatric treatment, leading the cardiologist to prescribe medications that interact negatively with ones that she did not know the patient was taking for depression. Or an individual who abuses pain killers could possibly block access by his family doctor to information about previous drug abuse and even data revealing that other providers are concurrently providing controlled medications.

An EHR system that provides patients with granular control of personal health information will only be valuable and ethically defensible if it can support the goal of patient empowerment while also anticipating and addressing these possible problems. Therefore, the goal of this document is to describe the nature of the challenges facing those who would design and implement a system allowing granular control for patient clinical care, as well as to outline specific options for addressing the problems. The challenges are especially complex due to the relevance of three important values:

[d] This document focuses on patient control of electronic health records (EHRs), and not directly on Health Information Exchanges, since EHRs provide a more likely conduit through which patients can directly interact.

(1) maximizing patient autonomy and choice about access to personal health information by accommodating patient control over information,
(2) supporting quality medical care in the best interests of the patient,
(3) valuing societal interests in an efficient health care system.

These values are important in their own right, but they also derive from long-standing, recognized principles of bioethics[14]:

(1) Respect for autonomy (requiring respect for the decision-making capacities of autonomous persons);
(2) Beneficence (requiring the promotion of the patient's best interests and overall well-being);
(3) Nonmaleficence (requiring the reduction or avoidance of harm to others); and
(4) Justice (requiring fair and appropriate distribution of benefits, risks, and costs).

Describing principles and the guidance that follows, however, will not always be sufficient. Classic questions in medical ethics have arisen, for instance, in situations where it is impossible to maximize both respect for autonomy and beneficence. As with any ethical principles or values, these are only useful if they can be applied in specific ways to help understand and explicate moral issues. One often would be aided by some sort of "user's guide" for applying them and accommodating conflicts among them.

The approach adopted here is to create a "Points to Consider" document, a model that has been successfully used in other settings to guide policy decisions and design choices that raise thorny ethical, regulatory, and policy questions.[15, 16] We provide an overview of the benefits, risks and challenges of granular control of EHRs; a review of the key ethical principles, values, and Fair Information Practices that ought to guide development of an EHR that accommodates granular control, and offer seven detailed Points to Consider to guide decision making.

A. The Benefits, Risks, and Challenges of Granular Control of EHRs

Electronic health records (EHRs) are becoming common in medicine and will most likely become "standard of care" in the future. Massive amounts of patient data, which will soon

include genetic test results and other genomic data, will probably become part of a future EHR offering the potential to improve the quality of health care and lower its costs. Paper records can impede efficient sharing among health care providers, leading doctors to practice without the benefit of information about their patients that may exist elsewhere, resulting in duplication of tests and treatments and sometimes in avoidable negative outcomes.[17, 18] In addition, a comprehensive EHR could allow evaluation of care and outcomes in ways that are unthinkable with paper records, for example, by making it possible to tie reimbursement to systems of care and outcomes rather than to services rendered.[19-21] The federal government is funding research and development to improve and link EHRs and to support adoption in clinical practice through measures such as the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009.

Quite apart from any system benefits, EHRs represent an important opportunity for more comprehensive involvement by patients in their care. In much the same way that informed consent practices changed over the past three decades to ensure that patients could better understand medical information being provided to them, patient-controlled EHRs are expected to empower patients by giving them greater control and more effective access over their medical information.[1] Thus, exercising control – even granular, detailed control – may have both instrumental and symbolic value to patients. Yet, were patient empowerment the only value worth supporting, granular control of EHRs would likely be reduced to a technical challenge of providing appropriate means for enabling patients to interface with a computer to effect their wishes. For patients, however, as we discuss throughout this document, granular control involves more than the mere technical manipulation of information; it involves expressions of their preferences and values about the management of personal health information, and about their trust in the security and integrity of EHR systems and the veracity of the data they contain.[1, 13, 22]

But while the power to control information offers obvious benefits, it also raises new concerns and intensifies old ones, perhaps most importantly related to privacy and security. Many have pointed out that a comprehensive EHR that can be accessed by all of a patient's health care providers (which includes potentially hundreds of authorized individuals), at any time, may lead to undesirable consequences.[22-24] For example, some information is embarrassing to patients and knowing that a seemingly endless list of persons involved in their

clinical care may learn such information may make a patient uncomfortable, perhaps to the point of no longer seeking health care.[13, 22]

Information in the EHR, such as the fact that an individual once tested positive for a sexually transmitted infection (STI) or was treated for depression, also may fuel irrational biases in providers. After all, personal health information may include intimate details about an individual, so the prospect of that information being available broadly can be daunting. In a 2010 national survey, the California HealthCare Foundation found that 15% of adults said they would withhold information from their doctor if they knew the information would be shared, and another 33% said they would consider withholding information.[22] Similarly, a 2010 study by the Markle Foundation found that 79% of those surveyed thought patients should be able to review who has had access to their personal health information, and the same percentage thought individual patients should be able to make informed choices about how their information is collected, shared, and used. Over 70% of doctors also agreed with both these statements.[25] In multiple studies since 1990, a majority of the public has consistently expressed concerns about health information privacy and security.[26]

At the same time, it is easy to envision ways that granular control could interfere with a physicians' ability to provide appropriate care. A system of granular control that blocks health care professionals from accessing possibly lifesaving information – for example in emergency situations, where a patient is unconscious or incapacitated or there is limited time for discussion – would be particularly problematic, especially if this is information that the patient would have wanted them to see. Such a system would be unacceptable. Helping patients intelligently exercise granular control requires educating them about the meaning of the information that exists in the EHR and how health care providers use it.

This can be difficult even for educated individuals, let alone for those who have limited education or literacy. Studies have shown that a majority of patients fail to understand simple medical terms appearing in medical records, such as "fracture" or "sprain," and even college educated patients have trouble understanding basic statistics used in medicine.[27, 28] Further, there are important questions regarding how to group information in ways that would allow patients to make decisions regarding what information physicians can access. A system that would provide the finest level of granularity might list each specific piece of data (such as a blood test result), including the result of each observation or conclusion recorded by a physician,

and each test and treatment performed, and their outcomes, at each date of service. A system providing more generic granular control might group such data by disease type or provider type, and limit which potential health care providers could view each group of data. Both types of systems (i.e., one with the finest granularity versus one with more generic choices) may be ethically defensible, but their impact will differ significantly.

It should come as no surprise that the potential benefits and risks arising from providing patients with varying levels of control over personal health information has led to sustained discussion over the past several years. It was with this in mind that the National Committee on Vital and Health Statistics (NCVHS) in HHS and the PCAST took up the topic,[2, 29-31] and why a set of research projects have been funded by the ONC.[3] This document is being prepared as part of a grant to the Indiana Health Information Technology that includes support to develop a prototype technology for providing patients with granular control. The success of such projects will depend on identifying and addressing important challenges that accompany any attempt to provide patients with granular control.

B. Principles of Bioethics and Fair Information Practices (FIPs)

Applying bioethics principles is an important strategy to understand and address moral problems in health care. While differences over the content and number of principles varies among commentators,[32] a consensus has formed around the need to respect patient autonomy, promote patient well-being, minimize harm, and ensure fairness.[33-39] The main principle favoring patient granular control is *respect for autonomy*, interpreted generally as a precept to provide patients with the ability and opportunity to control the nature and form of the health care they receive, mainly by being sufficiently knowledgeable to make informed decisions. Respect for autonomy is the basis for informed consent and shared decision making in modern health care.[4] It is a logical step, then, to conclude that patients should be able control how information about them is accessed and disclosed. The patient can decide generally whether to go to the doctor, which doctor to go to, what to tell the doctor, and what tests or treatments to undergo. By the same reasoning, it might seem, the patient should also have a say in what data about himself or herself that doctor should be able to view in the health care record.

At the same time, it is essential to acknowledge and address the risks that a patient exercising granular control might be exposed to by leading a health care provider to practice

without crucial information. Many patients may be unaware of how limiting the information obtained by some future physician could lead to avoidable harms. For example, information about a rash that a patient had one year ago could hold the clue to a diagnosis in the following year, and thus the patient who makes his dermatological information available only to dermatologists may undergo unnecessary testing, misdiagnosis, and resulting harms or even death. Even physicians may be unable to anticipate how one piece of information could be helpful later. These examples might be construed to suggest that there is a zero-sum trade off at work: where giving patients significant personal control (and thus maximizing their autonomous decision making power) can *only* come at the expense of promoting their own welfare (and thus at the expense of beneficence); or that the only way that physicians can care for and treat patients is to override the patient's demonstrable interests in having control over information about them. Such a characterization of a stark "conflict" between the principles poorly reflects reality and is bad philosophy.

At the same time, portraying respect for autonomy and beneficence as opposing principles is a mistake. Just as it would be presumptuous and patronizing to restrict patient control on grounds that they "can't understand," so too might offering patients too many choices in an unclear or unorganized way lead to confusion and thus undermine, rather than enhance, the exercise of autonomy.[40-42] In general, a system should be structured to help patients understand the possible benefits and risks of restricting access to their information and encourage them to reflect on their preferences and goals in seeking health care when deciding what information in the EHR to share and with whom.

Beyond respect for autonomy and beneficence, the principle of justice is reflected in the value society places in an efficient health care system and in the appropriate distribution of risk and benefit. Considerations of fairness and non-discrimination and about effective and efficient use of resources play a role in the conversation about how to design an EHR system that offers granular control. There are ways that unrestricted granular control by patients could conceivably violate legal and regulatory requirements – such as mandated disclosure of STIs – that are based on public health requirements that place the community's well-being above that of any one individual.[43] Providing granular control will inevitably raise tensions between what is respectful of individual autonomy and what is fair to the broader community.

In addition to these bioethics principles, any system of granular control must be consistent with Fair Information Practices (FIPs), a set of principles that protect individual informational privacy with respect to electronic record systems. FIPs were first introduced in 1973 and served as the basis of informational privacy laws enacted in the US (most notably, the Privacy Act of 1974) and omnibus privacy legislation in many European countries.[44, 45] The ONC has formulated a set of FIPs specifically for Health Information Exchanges which map well onto bioethics principles (see Appendix One). Our focus in this document will be on bioethics, as reflected in ethical principles and in FIPs, postponing closer examination of legal issues for another setting. In addition, many ethical issues may exist independently of legal restrictions.

C. Points to Consider

These Points to Consider are written as a set questions that should be addressed by anyone involved in designing, implementing, or evaluating a system that provides patients with granular control. After each question, we provide a discussion of the issues involved and the options available for the design of a system of granular control. Each discussion includes the following sections:

- a key question that frames the ethical problem;
- a description of the challenges involved in answering the question;
- a list of options available to answer the question;
- a discussion of the issues and applicable principles of bioethics and FIPs that each option generates.

We aim to avoid identifying a single option or approach as the "correct" response to the question involved in each Point. Instead, the discussion that follows each Point is meant to guide designers through the issues they must face in any system of granular control. This Points to Consider document aims to present options that may be available in many different types of EHRs, given the variety that exist across the country, but it is possible that some described options may not be possible for some EHRs. In addition, as EHRs develop over time, some Points may need to be revisited in the future in light of technological or policy developments.

1. **How will the system make transparent the uses and flows of clinical information so that patients can make informed choices about disclosing/restricting their information?**
   (Applicable bioethics principle: respect for autonomy;
   Applicable FIPs: openness and transparency; individual choice)

a. Challenge

This question encompasses at least three interconnected issues:

i. How will patients be told about the flows, uses, and users of their health information?
ii. How will patients learn what information is contained in their EHR so they can appreciate what they are granting access to – a prerequisite for individual choices to be meaningful?
iii. How will patients be assisted in understanding the meaning of the medical information in their EHR (e.g., terminology used in pathology, laboratory, radiological tests/reports)?

The challenge is to make it possible for patients to understand enough about the EHR so that they can make good decisions about access to their personal information, even if they do not fully understand the clinical information or all the possible uses of the EHR.

It will be important to decide how patients should be informed about the flows and uses of their clinical information. And such descriptions can be very complex. For instance, patients could be told that their clinical information might be seen by myriad people (including clinicians of many different types, nurses, public health authorities, dieticians, home health care providers, and physical, rehabilitation, or respiratory therapists) at many different institutions (including laboratories, pharmacies, long-term care facilities, hospitals, and ambulatory care centers). Unless a patient is allowed to see what is in their own EHR, it will be difficult (perhaps profoundly so) to decide about any access restrictions. Unless they understand what information is in the EHR their decisions cannot be fully informed.

b. Options for Providing Information to Patients

i. Provide no education regarding what information exists in the EHR or the flow and uses of information besides the required, and fairly general, Notice of Privacy Practices. Patients will utilize whatever additional understanding they happen to have, including any misunderstanding, in exercising granular control.

ii. Provide educational materials for patients to review before exercising granular control. These materials can be more or less specific or customizable to the literacy and interests of different patients.
iii. Give all patients access to a trained educator or practitioner who can brief or tutor them on the EHR.

c. Issues and Principles

Option (i) appears to fail to respect the principle of respect for autonomy. Patients who do not understand the information in their EHR, or are not told who may use it, may make choices about access that have little to do with their true preferences. For example, consider a patient who wishes to withhold from their endocrinologist medical information collected by a dermatologist believing (incorrectly) that the information from one specialist is not needed by the other. Or perhaps the patient was concerned about an embarrassing fact being disclosed. In the absence of understanding why it would be in their medical best interest to have this information shared, the patient may exercise choice, but may hardly be considered to be expressing their autonomy. Option (i) likely fails to respect the principle of beneficence. By leaving patients uneducated regarding the issues involved in exercising granular control, this approach threatens the well-being of patients who choose to restrict access of health care practitioners. While some patients will have adequate information to make informed choices, designing a system using Option (i) here appears to threaten the well-being of many who are uneducated or unaware. If, on the other hand, patients are helped to understand the need for many specialists to have access to the same information, it may be possible for patients to exercise their autonomy and receive medical care that serves their best interests.

Option (ii) is more attractive than Option (i) insofar as it is more consistent with the principles of respecting autonomy (by providing more information to enable informed choice) and promoting beneficence (by encouraging more engagement with health care providers). However, there are significant challenges to determining what sort of educational materials to provide, their format, how to tailor them to different levels of ability and interest, and how to evaluate the effects. Each patient would have to get at least a baseline of information that accurately describes the potential risks involved in restricting access to information but does not do so in such a way that unfairly or misleadingly dissuades patients from ever exercising

granular control. Similar considerations apply to whether materials are provided at the physician's office, what format those materials are in, and who provides them to the patient.

Option (iii) may seem the most attractive option given that it would highly promote both respect for autonomy and beneficence. Indeed, face-to-face counseling could supplement Option (ii)[46]; however, as a matter of justice, and in particular the fair distribution of overall resources, the availability of and access to trained individuals may be a cost the health care system is not prepared to cover.

2. How will the system structure the array of choices patients can specify for disclosure and non-disclosure of their clinical information?

(Applicable bioethics principle: respect for autonomy;
Applicable FIPs: openness and transparency; individual choice)

a. Challenge:

One way to envision how a system would offer granular control to patients is by listing the sort of information that exists in the EHR, possibly grouped in various ways, and asking whether specific providers may access that data. A central question for any system to provide patients with granular control is whether and how to group clinical information when offering patients the choice of restricting access to that information by health care providers. A separate, but equally critical question, is whether and how to group providers who may be granted access (or not) to specific parts of the patient's EHR. For instance, patients may be given the option of identifying providers individually (e.g. by name), or by practice group, institution, or specialty.

The options presented under this Point (Section b., next) involve choices regarding whether and how to focus on the question of regarding how to group the information in the EHR when offering patients the option of determining access to that information by providers. We do not explicitly discuss the options for grouping the list of possible providers who may access each of those pieces of data (or types of data), although we discuss this issue in the section on Issues and Principles (Section c.), below.

b. Options for Presenting Personal Health Information

i. List each specific piece of information, including the result of each observation or conclusion recorded by a physician, and each test and treatment performed, and their outcomes, at each date of service. Then the patient could decide, for each piece of information, whether each potential health care provider could view that piece of information.

ii. Group information in various ways, reducing the granularity of patient control, for instance grouping according to:

   a. Date of service: e.g., all data collected on January 16, 2011,
   b. Provider: e.g., all data, including ordering of tests by providers,
   c. Disease: e.g., all data relating to diabetes,
   d. Treatment: e.g., all data related to a specific prescription drug or treatment plan,
   e. Area of medical care: e.g., all data related to endocrinology, or
   f. Sensitivity of the information, as recommended by the NCVHS: e.g., in predetermined/predefined categories like reproductive health, mental health, substance abuse, domestic violence, and genetic information.[31]

iii. Present choices that encompass a compromise between Options i and ii above, where the system allows granular control choices at a predetermined standardized level of granularity (as in ii, above), but considers accommodating additional requests for restrictions on a non-standardized basis.

c. Issues and Principles

Option (i) provides control at the finest level of granularity. In so doing, it provides the greatest degree of patient control and empowerment. At the same time, this approach could be the most challenging to comprehend by patients. A list of each individual note, prescription, test result, etc., issued on each interaction with the health care system would be understandably overwhelming. How would a patient decide whether his cardiologist needs to have access to the complete blood count (CBC) drawn in January 2012 by his internist? Is the choice different for the complete metabolic panel (CMP) drawn on the same day? How about the chest x-ray that was performed? Systems that provide an abundance of poorly defined choices to patients fail to respect autonomy. Maximizing choices is not necessarily a way of maximizing patient autonomy.[47] Option (i) might also lead to negative outcomes and thus fail to respect the

principle of beneficence. A patient with too many choices – especially one without the benefit of education or transparency – may be unable to act in their own best interest. Where an informed patient may be able to manage well with finely granular choices, other patients may be overwhelmed. Option (i) would thus be most appropriate when accompanied by the kind of detailed education described in Point 1 above.

Option (ii) could reduce the risks in Option (i) by grouping the information in various ways. The trade off is that any such grouping reduces the ability of a patient to make the most fine discriminations about the use of their information, but does so in a way that limits the type of control into more manageable chunks. For instance, if a system was organized by Option (ii.a) a patient could not choose to restrict access by his cardiologist to one test (e.g., his HIV test, perhaps done on January 16, 2012) without also restricting access to other tests (e.g., his chest X-ray). Thus, grouping information according to Option (ii) reduces the number of choices available to the patient, but in so doing, it promotes patient autonomy by providing choices that are more comprehensible (and through which the patient could best express his or her desire for privacy weighed against possible negative consequences), and serves to promote their clinical best interests (beneficence).

That said, Option (ii) can be critiqued due to its failure to provide the sort of fine granular control that some patients may desire. For example, under this system, there may be no mechanism to restrict access to a single note or set of tests or treatments, as is provided by Option (i).

Option (iii) attempts to accommodate patients who will desire to make some access restriction choices at a coarser level of granular control, as in Option (ii), and others at a finer level of control, as in Option (i). This option could be seen as maximizing patient autonomy by providing the ability for the patient to determine the level of granularity that he or she desires for a specific situation. At the same time, this represents a level of complexity – asking patients to determine the level of granularity as well as the specific questions about access – that may be overwhelming. And a system that overwhelms patients with complexity will fail to fulfill the goal of respecting autonomy or beneficence.

The discussion so far has focused on the granularity of the control that patients may exercise for their data, i.e. on a finer level (e.g., by specific observation or test result) or more generally (e.g., by disease). A related issue involves the granularity of control over which

patients can define which providers can view a given piece of data. The finest level of granularity for this determination would be for the patient to define, for each specific, named provider whether he or she can view the data in question. But providers could also be grouped: a patient may decide what can be viewed by all the providers in one practice group, or who will see the patient in a certain time period, or in one specialty. Questions related to how patients will define which providers can have access to specific parts of the patient's EHR are of course central to a system of granular control. In fact, a patient may choose to give specific providers access to all the information in the EHR, or at least all the information resulting from a type of care, expressing trust in those providers or their institution.

This possibility is consistent with the idea that patients might be more able to express their autonomy by focusing on the individuals and institutions that would use or access their information rather than the information itself. This is consistent with the notion that patients are prepared to forgo some control when they believe that others will responsibly use the information in a trustworthy manner.[48]

It is likely that different levels of granularity, regarding data or providers, may be appropriate for different patients or situations. It is unlikely that a "one size fits all" approach to granular control could accommodate their desires to restrict their health information. The question is whether the system should be designed to accommodate what might be maximally desirable in terms of patient autonomy (bearing in mind that a broad array of choices may not maximize autonomy), or be designed to provide fewer choices for granular control, but which may contribute more to an efficient system of health care delivery. And, clearly, the possible level of granularity may be limited by what is technically feasible. This is why we emphasize that the use of the Points to Consider should not be approached as a "one time only" exercise, but also should be used to evaluate how well the issues addressed are being managed in an ongoing process.

3. **How will technologically and/or medically unsophisticated patients, or those with other challenges, exercise their choices for granular control of their information?**
   (*Applicable bioethics principle: respect for autonomy;*
   Applicable FIP: individual access)

a. Challenge

This question addresses issues not only of technological literacy (such as understanding how computers collect and store information, how data might be encrypted, etc.), but medical literacy, reading and English literacy. It will be important to consider different methods of recording patients' choices, given that the patient population spans all technological skill levels, as well as all physical, language, and mental abilities. Finding a "one size fits all" solution to register access preferences is unlikely to accommodate all patients. On the other hand, it could constitute a significant expenditure to accommodate each patient's specific needs. That said, there is an ethical obligation to ensure that the exercise of rights or privileges is not dependent on one's ability to read/speak English, understand medical terminology, or be able to use a computer.

b. Options for Exercising Choice

Because the overall goal is to allow patients to express and record their information-sharing preferences, it is important that the options for doing so span a reasonably broad range of patient capabilities. In this case, that may mean that the system should be designed to accommodate various input methods. For instance, the system could:

i. Provide an electronic input option for choices to be recorded by the patient (and/or his representative) only, and be available in a variety of languages (at least English and Spanish);

ii. Devise a two-step process for input, giving patients a paper form containing the choices available, which is then taken by a medical staff member to be recorded in the electronic system;

iii. Provide other means for patients to learn about their options and indicate their preferences, for instance through discussion with a medical staff member (e.g., for those who have difficulty reading, or are sight-challenged) who would then record the patient's choices and preferences.

c. Issues and Principles

The options are far from exclusive: while a computer-based system would be desirable for those who are able to use it effectively, patients who are not (for one of the reasons listed)

should be accommodated in some other way (as in Options ii and iii). The ethical basis for this variety is based on the principles of ethics and fair information practices that support a system of granular control for all patients, independent of their abilities to use a computer. In addition, it would seem that the sort of educational activities discussed under Point 1 would need to be adjusted, if possible, based on the abilities and desires of patients.

Finally, making the system of granular control accessible to those who speak languages other than English makes good sense. Although HIPAA does not require health care providers or facilities to furnish translations of their Notice of Privacy Practices document, in many instances Title IV of the Civil Rights Act of 1964 might require translations. Indeed, there is a career subspecialty for medical translators/interpreters who provide translation services to patients with limited English proficiency.[49]

4. How will the system inform *providers* of a patient's preferences for data access/restrictions?

(Applicable bioethics principles: respect for autonomy, beneficence; Applicable FIP: Collection, use, and disclosure limitation)

a. Challenge

For providers to act in the patient's best medical interest (thereby promoting beneficence) they need to know all relevant information about the patient. Incomplete information may mean an incorrect diagnosis or an inadequate treatment plan. In the worst case scenario, a patient who opts out of having an EHR may put themselves in the position of denying physicians access to important information. On the other hand a patient who's EHR is incomplete presents challenges for accurate diagnosis and treatment.

But providers also have an interest in building and maintaining a relationship of trust, one in which patients have a role in deciding about their care and about the use of information about themselves stored in the EHR. The trust relationship, however, goes both ways: just as a patient is entitled to know what the reasons are that a provider is recommending a treatment, so is a provider entitled to believe s/he deserves to be informed when information is being withheld. In addition, a provider might want to understand how and why patients decide to restrict and/or share access to their medical information.

b. Options

i. When a physician views the patient's EHR, the system will specify which information exists and is accessible, and which information exists but is being restricted due to the patient's prior preferences and privacy settings.

ii. When a physician views the patient's EHR, the system will only display the information that is allowed by the privacy settings, without disclosing the existence of other information that is subject to access restrictions.

iii. When a physician views the patient's EHR, a broad statement that information has been restricted would be provided without specifying which types of information are not accessible.

c. Issues and Principles

Some designers of a system of granular control might favor Option (i), arguing that even though patients have a right to restrict who sees their data, doctors should be informed when information is present in the EHR but not being displayed. Informing physicians of the type of information that is restricted would allow physicians to discuss those preferences with patients and discuss the provider's viewpoints on restricted access. The goal of this approach would be to inform physicians that they are practicing without all the information contained in the EHR; arguably, though, this option may violate the patient's very point in requesting privacy. Moreover, some federal and state regulations (e.g., 42 CFR Part 2) require confidentiality for sensitive medical information (e.g., information maintained and shared by federally supported substance abuse programs), and do not allow providers to give notification that the information exists when sending a patient's record without the sensitive information.

Option (i) might also help avoid the problem of a physician becoming concerned about why a specific test or a recommended treatment was not ordered in the past. For example, if the physician knows that the patient had a broken bone in the past, but is being told by the radiology section of the EMR that there is no information about an x-ray being performed, he may be uncertain as to whether the information exists but is restricted, or does not exist at all.

At the same time, one could argue against Option (i), and for Options (ii) or (iii), by pointing out that there are very few, if any, circumstances in which doctors now practice

medicine with full information – certainly not with a paper-based record system. Further, given that patients are always ultimately in control of the information they decide to communicate to (or withhold from) their providers, one could conclude that a patient's decision to restrict access to data in the EHR need not be disclosed.

If Option (i) is chosen, another decision would involve whether to disclose that the restricted access is due to the patient's choice, or if the cause should be left vague. Vagueness in this area has the advantage of perhaps diminishing the chance that the physician will directly pressure the patient for access or refuse to treat unless provided access. At the same time, physicians seeing this notification, no matter how vague, may intuit the cause.

Option (ii) has the advantage of avoiding physician pressure on the patient to reveal information the patient does not want revealed, or of the physician treating the patient with suspicion (or even annoyance) over knowing some information is being restricted. This option also allows the patient to maintain the access controls s/he prefers, although it might also oblige providers to make additional inquiries of patients.

Option (iii) would have a similar effect on physicians, in that they would be alerted to the fact that not all information available in the EHR was available to them. It might provide the opening for a more detailed conversation with the patient, or it might inhibit the ongoing relationship.

5. Under what circumstances/conditions will the system allow health care providers to access patient data in ways that may over-ride stated preferences for granular control? *(Applicable bioethics principles: respect for autonomy, beneficence)*

a. Challenge

A situation in which the benefits of the EHR are perhaps best displayed is when an unconscious patient is brought into the emergency room, and doctors are able to use the EHR to find out that the patient has a certain disease or is taking a certain drug. Having access to an EHR in this sort of case can save the patient's life. Reality is perhaps rarely this simple: emergency room personnel often do not have time to refer to the EHR until after a patient has been stabilized. In any event, the ethical question in an emergency situation is whether the patient's

data should be accessed in ways that might override their prior stated preferences for limiting access to the EHR, and if so, how the facts of that access should be accounted for or tracked.

It is also possible that even in non-emergency situations, health care professionals could have good reasons to want to override restrictions on access to information in the EHR; for example, a patient may present to an emergency room incapacitated and unable to consent to disclosing all of their health information. In another example, a physician who is considering prescribing a controlled medication, but has not been given access to a patient's full record, might wish to override some limits. The issue in this Point is whether there are circumstances in which, during an emergency or typical clinical encounter, a patient's preferences might need to be overridden, and what those circumstances might be. It should be pointed out that federal regulations (42 CFR § 2.51(a)) *permit* disclosures of protected substance abuse treatment information without patient consent in a medical emergency, as long as the emergency poses an immediate threat to the patient's health and requires immediate medical intervention. Similarly, disclosures of protected substance abuse treatment information without patient consent are *permitted* to the Food and Drug Administration (FDA) when it asserts that a patient's health might be in jeopardy due to an error in the labeling, manufacture, or sale of a product under FDA's jurisdiction, and the information is only used to notify patients or physicians of the potential dangers (42 CFR § 2.51(b)). Similar emergency exceptions exist within state laws that restrict the disclosure of certain types of health information.

b. Options

i. Never allow providers to override stated patient preferences for granular control, even in emergency situations where access to restricted data in the EHR could save the patient's life.

ii. Allow providers to override stated patient preferences for granular control only in emergency situations, where access to data could be life saving, but not in other serious but non-life-threatening situations, where the patient could be asked for access permission.

iii. Override patient preferences in non-emergency situations, but only under pre-determined, specified circumstances.

iv. Override patient preferences in non-emergency situations in any circumstances where the provider believes the patient's best interest will be served by accessing otherwise restricted data, with a requirement that a justification be added to the patient's EHR afterwards.

c. Issues and Principles

The ethical principle of respect for autonomy motivates Option (i). In contrast, Option (ii) is motivated by the ethical principle of beneficence, based on the argument that the welfare of the patient outweighs the importance of respecting the patient's stated preferences.

Complicating this way of parsing the ethics is the possibility that most patients would want their stated preferences for granular control to be overridden in emergency or life-threatening situations (or that emergency situations should be exempt from their stated preferences). From this perspective, even Option (ii) could be supported by the principle of respect for autonomy.

At the same time, a justification of Option (ii) based on respect for autonomy might militate for asking patients ahead of time, when they are stating their desire for granular control, how they wish doctors to act in emergency situations. At the same time, even if a patient says that he or she wants access restrictions to remain in place, even in life threatening situations, it may be hard to believe that this truly represents a patient's true desires.

Under Option (iii) a set of non-emergency situations should be specified in advance under which preferences will be overridden, with a specific rationale for each. The ethical justification for taking the time and effort to predetermine these circumstances is that honoring patients' preferences is still the primary objective, but also taking into account clinical situations in which the patient's best clinical interests will be served by overriding their preferences only when absolutely necessary. A new patient coming to a doctor for pain medications might be such a situation.

Option (iv) takes Option (iii) further, but instead of having a pre-determined set of non-emergency circumstances in which preferences are overridden, the provider makes that determination at the time of the clinical encounter. This would also encompass the provider who prefers to treat only patients who have not restricted access to any part of their record. Many

would argue that this option would unacceptably violate the autonomy of patients and would make any system of granular control almost pointless.

Under all of these options, it is ethically necessary in order to fulfill the obligation of respect for persons, to inform patients of whatever option is implemented. Moreover, patients should be informed *before* such a circumstance might arise. For instance, the provider should have a stated policy covering their approach under this circumstance (whether it is Option i, ii, iii, or iv); if Option iii, a general description of the type of specific reasons patient choices would be overridden should be provided to patients; and if Option iv, a clear notification to patients should be provided up front, so they can determine whether they accept the doctor's policy, or whether they prefer to seek treatment elsewhere. Finally, Options ii, iii, and iv could be coupled with a system for auditing any such overrides to evaluate the severity of the situation and the reasonableness of the provider's decision to override patient access preferences. Indeed, 42 CFR § 2.51(c) requires that immediately following a disclosure of covered substance abuse treatment information made for a medical emergency, the name and affiliation of the medical personnel to whom the disclosure was made, the individual making the disclosure, the date and time of the disclosure, and the nature of the emergency that required the disclosure be documented.

6. How will patients be told about mandatory reporting requirements (e.g., public health, gunshots, abuse, disease registries, etc) and their impact on granular control?
(Applicable bioethics principles: respect for autonomy, beneficence;
Applicable FIP: openness and transparency, individual choice)

a. Challenge

Federal and/or state laws require that medical information pertaining to a possible criminal activity (e.g., child abuse or neglect, domestic violence, and gunshot wounds) be reported to the appropriate authorities. Similarly, when a patient with a communicable disease presents for treatment (whether for that condition or something unrelated), state and/or federal laws/regulations often require reporting of identifiable health information about the disease. Because of this, patients will not be able to exert granular control on such information. Any system of granular control must anticipate and address this issue. For instance, it may seem

appropriate to inform patients of the requirements for disclosure and the ways in which stated desires for granular control would be over-ridden by such requirements.

b. Options for Disclosing Mandatory Reporting Requirements

Legal requirements must, of course, be respected once a diagnosis of a reportable disease is made. However, a system of granular control might inform patients of the existence of such legal requirements and how they will impact disclosure, in the following ways:

i. Do not explicitly inform patients regarding legally mandated reporting requirements (i.e., that irrespective of her desire to restrict disclosure, some circumstances mandate disclosures).

ii. Provide a general explanation that there may be legal reasons why some personal health information must be disclosed, but do not detail those reasons. This could include, for example, putting posters in patient intake areas in clinics, physicians' offices, hospitals, outpatient facilities, etc., or very general statements in Notices of Privacy Practices given to patients.

iii. Inform patients more specifically what sort of situations would require disclosure of personal health information to public health authorities and/or law enforcement (e.g., STIs, communicable diseases, epidemic and/or pandemic outbreaks, abuse, gunshots, suspected bioterrorism), and what sort of information would be disclosed (e.g., name, address, diagnosis, etc.).

c. Issues and Principles

The HIPAA Privacy Rule requires that Notices of Privacy Practices describe the ways that the providers are allowed to use and disclose health information, including mandatory disclosures, although notices might not distinguish between what information disclosures are mandatory versus those that are otherwise allowed without patient authorization.[(50)] So, for some organizations, Option (i) could represent the status quo. Ethically, however, one could argue that it is more appropriate to at least provide patients with some details about such requirements, especially if one is also offering choices regarding granular control. That leaves Options ii and iii, which disclose varying degrees of detail about mandatory reporting requirements.

At the same time, such information, and the more specific information provided under Option (iii) might dissuade a small minority of patients from seeking treatment for a reportable condition. One might argue that allowing such choices by patients reflects respect for autonomy, though that could be questioned in at least some situations. (Is it ethical to make sure a parent who is abusing their child knows the danger of bringing that child to the emergency room? How about a patient who has been shot?) If a practitioner has a reason to suspect that a particular patient might not seek treatment, or might pose an imminent risk to the public health and/or safety, then under the ethical principle of beneficence (doing what is best for the patient, and in this case, what may also be best for a child or society at large), the provider might wish to withhold information about the specific nature of mandatory disclosures from the patient. However, such cases should be the exception, not the rule.

Appendix One

Fair Information Practices for Health Information Exchange (ONC's FIPs) mapped with Bioethics Principles

Individual Access • ***Respect for autonomy***	Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format.
Correction • ***Respect for autonomy*** • ***Beneficence***	Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information, and to have erroneous information corrected or to have a dispute documented if their requests are denied.
Openness and Transparency • ***Respect for autonomy***	There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information.
Individual choice • ***Respect for autonomy***	Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use and disclosure of their individually identifiable health information.
Collection, Use, and Disclosure Limitation • ***Nonmaleficence***	Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified lawful purpose(s) and never to discriminate inappropriately.
Data Integrity and Quality • ***Nonmaleficence*** • ***Beneficence***	Persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.
Safeguards • ***Nonmaleficence*** • ***Beneficence***	Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use or disclosure.
Accountability • ***Nonmaleficence*** • ***Beneficence***	These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.

(Source: Office of the National Coordinator for Health Information Technology. Nationwide privacy and security framework for electronic exchange of individually identifiable health information. ONC. December 15, 2008)

References

1. Health IT Policy Committee, Privacy and Security Tiger Team. Letter to David Blumenthal, Chairman of the Office of the National Coordinator for Health IT, August 19, 2010 [cited 2012 February 15]. Available from: http://healthit.hhs.gov/portal/server.pt/document/947492/tigerteamrecommendationletter8-17_2_pdf.
2. President's Council of Advisors on Science & Technology (PCAST). Report to the President realizing the full potential of health information technology to improve healthcare for Americans: a path forward. PCAST, Excutive Office of the President, U.S. Washington, D.C.; 2010. 108 p [cited 2012 February 15]. Available from: http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf.
3. Office of the National Coordinator for Health Information Technology (ONC). Health Information Exchange Challenge Grant Program. ONC, U.S. Department of Health and Human Services; 2011 [cited 2012 February 15]. Available from: http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=3378.
4. Faden R, Beauchamp T. A history and theory of informed consent. New York: Oxford University Press; 1986. 392 p.
5. Katz J. The silent world of doctor and patient. Baltimore: Johns Hopkins University Press; 1984. 263 p.
6. Emanuel EJ, Emanuel LL. Four models of the physician-patient relationship. JAMA. 1992 Apr 22-29;267(16):2221-6.
7. Savulescu J. Rational non-interventional paternalism: why doctors ought to make judgments of what is best for their patients. J Med Ethics. 1995 Dec;21(6):327-31.
8. Quill TE, Brody H. Physician recommendations and patient autonomy: finding a balance between physician power and patient choice. Ann Intern Med. 1996 Nov 1;125(9):763-9.
9. Kon AA. The shared decision-making continuum. JAMA. 2010 Aug 25;304(8):903-4.
10. McNutt RA. Shared medical decision making: problems, process, progress. JAMA. 2004 Nov 24;292(20):2516-8.
11. Organization of Economic Cooperation and Development (OECD). Guidelines on the protection of privacy and transborder flows of personal data. OECD; 1980 Sep 23 [cited 2012 Feb 15]. Available from: http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html.
12. Office of the National Coordinator for Health Information Technology (ONC). Nationwide privacy and security framework for electronic exchange of individually identifiable health information. ONC, U.S. Department of Health and Human Services; 2008 Dec 15 [cited 2012 Feb 15]. Available from: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_0_18/NationwidePS_Framework-5.pdf.
13. Goldstein M, Rein A. Data segmentation in electronic health information exchange: policy considerations and analysis. Privacy and Security Whitepaper Series 2010. ONC, U.S. Department of Health and Human Services; 2010 Sep 29 [cited 2012 Feb 15]. Available from: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_950145_0_0_18/gwu-data-segmentation-final.pdf.

14. Beauchamp TL, Childress JF. Principles of biomedical ethics. 6th ed. New York: Oxford University Press; 2009. 417 p.
15. Estrin NF, editor. Medical device industry: science, technology, and regulation in a competitive environment. New York: Marcel Dekker, Inc.; 1990. 994 p.
16. Nail SL, Aikers MJ, editors. Development and manufacture of protein pharmaceuticals. New York: Kluwer Academic/Plenum Publishers; 2002. 462 p.
17. Chaudhry B, Wang J, Wu S, Maglione M, Mojica W, Roth E, Morton SC, Shekelle PG. Systematic review: impact of health information technology on quality, efficiency, and costs of medical care. Ann Intern Med. 2006 May 16;144(10):742-52.
18. Bates DW, Gawande AA. Improving safety with information technology. N Engl J Med. 2003 Jun 19;348(25):2526-34.
19. Bates DW, Ebell M, Gotlieb E, Zapp J, Mullins HC. A proposal for electronic medical records in U.S. primary care. J Am Med Inform Assoc. 2003 Jan-Feb;10(1):1-10.
20. Shortell SM, Casalino LP. Health care reform requires accountable care systems. JAMA. 2008 Jul 2;300(1):95-7.
21. Hillestad R, Bigelow J, Bower A, Girosi F, Meili R, Scoville R, Taylor R. Can electronic medical record systems transform health care? Potential health benefits, savings, and costs. Health Aff (Millwood). 2005 Sep-Oct;24(5):1103-17.
22. Californina Healthcare Foundation (CHCF). Consumers and health information technology: a national survey. Oakland: CHCF; 2010 April [cited 2012 Feb 15]. Available from: http://www.chcf.org/publications/2010/04/consumers-and-health-information-technology-a-national-survey.
23. Rothstein M. Debate over patient privacy controls in electronic health records. Bioethics Forum: Hastings Center; 2011 Feb 17 [cited 2012 Feb 15]. Available from: http://www.thehastingscenter.org/Bioethicsforum/Post.aspx?id=5139&blogid=140.
24. Alpert SA. Protecting medical privacy: challenges in the age of genetic information. Journal of Social Issues. 2003;59(2):301-22.
25. Markle Foundation. Markle survey on health in a networked life 2010. Markle Foundation; 2011Jan [cited 2012 Feb 15]. Available from: http://www.markle.org/sites/default/files/20110110_HINLSurveyBrief_1.pdf.
26. Westin A. What two decades of surveys tell us about privacy and HIT today. Health Privacy Summit. Washington, D.C., June 13, 2011 [cited 2012 Feb 15]. Available from: http://patientprivacyrights.org/wp-content/uploads/2011/06/AFW-SUMMIT-6-13-11.pdf.
27. Bagley CH, Hunter AR, Bacarese-Hamilton IA. Patients' misunderstanding of common orthopaedic terminology: the need for clarity. Ann R Coll Surg Engl. 2011 Jul;93(5):401-4.
28. Lipkus IM, Samsa G, Rimer BK. General performance on a numeracy scale among highly educated samples. Med Decis Making. 2001 Jan-Feb;21(1):37-44.
29. National Committee on Vital and Health Statistics (NCVHS). Letter to the Secretary - Recommendations regarding Privacy and Confidentiality in the Nationwide Health Information Network; June 22, 2006. NCVHS [cited 2012 Feb 15]. Available from: http://www.ncvhs.hhs.gov/060622lt.htm.
30. National Committee on Vital and Health Statistics (NCVHS). Letter to the Secretary, Individual control of sensitive health informaiton accessible via the Nationwide Health Informaiton Network for purposes of treatment; February 20, 2008. NCVHS [cited 2012 Feb 15]. Available from: http://ncvhs.hhs.gov/080220lt.pdf.

31. National Committee on Vital and Health Statistics (NCVHS). Letter to the Secretary - Recommendations regarding sensitive health information, November 10, 2010. NCVHS [cited 2012 Feb 15]. Available from: http://www.ncvhs.hhs.gov/101110lt.pdf.
32. Veatch RM. How many principles for bioethics? In: Ashcroft RE, Dawson A, Draper H, McMillan JR, editors. Principles of health care ethics, 2nd ed. West Sussex: John Wiley & Sons, Ltd.; 2007. p. 43-50.
33. National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. The Belmont report. Washington, DC: US Government Printing Office; 1979.
34. Gert B, Culver CM, Clouser KD. Bioethics: a return to fundamentals. New York: Oxford University Press; 1997. 320 p.
35. Beauchamp TL. The "four principles" approach to health care ethics. In: Ashcroft RE, Dawson A, H. Draper, McMillan JR, editors. Principles of health care ethics, 2nd ed. West Sussex: John WIley & Sons, Ltd.; 2007. p. 3-10.
36. Brody B. Life and death decision making. New York: Oxford University Press; 1988. 250 p.
37. Engelhardt HT. Foundations of bioethics, 2nd ed. New York: Oxford University Press; 1996. 446 p.
38. Ross WD. The right and the good. New York: Oxford University Press; 1930. 183 p.
39. Veatch R. A theory of medical ethics. New York: Basic Books; 1981. 378 p.
40. Manson N, O'Neill O. Rethinking informed consent in bioethics. Cambridge, New York: Cambridge University Press; 2007. 212 p.
41. O'Neill O. Autonomy and trust in bioethics. Cambridge, New York: Cambridge University Press; 2002. 213 p.
42. Zikmund-Fisher BJ, Fagerlin A, Ubel PA. A demonstration of "less can be more" in risk graphics. Med Decis Making. 2010 Nov-Dec;30(6):661-71.
43. Goodman KW. Ethics, information technology, and public health: new challenges for the clinician-patient relationship. The Journal of Law, Medicine & Ethics. 2010;38(1):58-63.
44. U.S. Department of Health, Education, & Welfare (HEW). Records, computers and the rights of citizens; report of the Secretary's Advisory Committee on Automated Personal Data Systems. Washington, D.C.: HEW; 1973 [cited 2012 Feb 15]. Available from: http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm.
45. Gellman R. Fair information practices: a basic history.Version 1.86; 2011 Oct 3 [cited 2012 Feb 15]. Available from: http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.
46. Coulter A, Ellins J. Effectiveness of strategies for informing, educating, and involving patients. BMJ. 2007 Jul 7;335(7609):24-7.
47. Schwartz P. Questioning the quantitative imperative: decision aids, prevention, and the ethics of disclosure. Hastings Center Report. 2011 Mar-Apr;41(2):30-9.
48. Kraetschmer N, Sharpe N, Urowitz S, Deber RB. How does trust affect patient preferences for participation in decision-making? Health Expect. 2004 Dec;7(4):317-26.
49. Civil Rights Act of 1964: Pub.L. 88-352, 78 Stat. 241, enacted July 2, 1964.
50. Standards for privacy of individually identifiable health information. Final Rule, 45 CFR parts 160, 162 and 164. Available 2012 Feb 15 from: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf.

*** List of Workshop Attendees:**

Denise Anthony
Associate Professor of Sociology
Research Director, Institute for Security, Technology and Society
Dartmouth College

Mike Burgess
Professor and Chair in Biomedical Ethics
W. Maurice Young Centre for Applied Ethics and the Department of Medical Genetics
University of British Columbia

Fred Cate
Distinguished Professor and C. Ben Dutton Professor of Law
Director of the Indiana University Center for Law, Ethics and Applied Research in Health Information (CLEAR)
Indiana University School of Law-Bloomington

Stanley Crosley
Of Counsel to Drinker Biddle & Reath
Director of the Indiana University Center for Law, Ethics and Applied Research in Health Information (CLEAR)

Ellen Fox
Chief Ethics in Health Care Officer
National Center for Ethics in Health Care
Veterans Health Administration

Ellie Garrett
Health Policy & Public Engagement Consultant

Jennifer Girod
Hall, Render, Killian, Heath & Lyman, P.C.
Indianapolis

Ken Goodman
UM Ethics Programs
University of Miami

Deven McGraw
Director of the Health Privacy Project
Center for Democracy & Technology

Joy Pritts
Chief Privacy Officer
Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services

Mark Rothstein
Herbert F. Boehl Chair of Law and Medicine
Institute for Bioethics, Health Policy and Law
University of Louisville

Additionally, comments were solicited from:

Robert Gellman
Privacy and Information Policy Consultant
Washington, DC