

The Autonomy Trap
The Privacy Symposium
Cambridge, MA, Aug. 24, 2007

Fred H. Cate

My title today—The Autonomy Trap—is taken from a 2000 *Connecticut Law Review* article by Professor Paul Schwartz.¹ In that and a series of related articles, Professor Schwartz lamented the extent to which privacy law in the United States and elsewhere had been reduced to a focus on individual control over personal data.

In the years since those articles appeared, the critique of bureaucratic privacy law has grown. Today it includes a chorus of scholars, government officials, and practitioners—including my cab driver on the way in from the airport. I want to touch on that criticism for just a moment this morning before focusing on the privacy of health information, where I fear the risks of getting snared in the autonomy trap are greatest and the risks to the public most severe.

The Focus on Consumer Control

Alan Westin in his groundbreaking 1967 study, *Privacy and Freedom*, defined privacy as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”² By the end of the 20th century, the focus on control had become the hallmark of data protection. In the words of the Supreme Court in the 1988 case, *Department of Justice v. Reporter’s Committee*, “both the common law and the literal understandings of privacy encompass the individual’s control of information concerning his or her person.”³

This is not just a U.S. phenomenon. It is plainly evident in the OECD 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*,⁴ the 1995 EU data protection directive,⁵ and APEC’s 2004 Privacy Framework, which provides that “[w]here appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information.”⁶

The problem with the focus on individual choice is that to date it has proved not only burdensome and unworkable in many settings, but often undesirable as well.

¹ Paul M. Schwartz, “Internet Privacy and the State, 32 *Connecticut Law Review* 815, 821 (2000).

² Alan F. Westin, *Privacy and Freedom* 7 (1967).

³ U.S. Department of Justice v. Reporter’s Committee, 489 U.S. 749, 763 (1988).

⁴ O.E.C.D. Doc. (C 58 final) (Oct. 1, 1980), at ¶ 7.

⁵ *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (Eur. O.J. 95/L281), Preamble, ¶ 25.

⁶ Asia-Pacific Economic Cooperation, *APEC Privacy Framework*, 2004/AMM/014rev1 (Nov. 2004), at 12.

The Focus on Notice and Choice

For example, the focus on choice has led to a migration away from substantive privacy protection towards procedural ones. For example, in 1999 Congress passed major financial privacy legislation as Title V of the Gramm-Leach-Bliley Financial Services Modernization Act.⁷ Ironically, Title V contains only three substantive restrictions on the use of personal information: prohibitions on sharing account numbers with third parties for marketing purposes, on pretext calling, and on transfers of personal information to third parties for marketing purposes if the data subject has opted out.

The real focus of the law is on procedural requirements. The law permits a financial institution to transfer any “nonpublic personal information” to nonaffiliated third parties only if the institution “clearly and conspicuously” provides consumers with a notice about its information disclosure policies and an opportunity to opt out of such transfers.⁸ That notice must be sent at least annually even if there is no change in its terms. The act provides many exceptions to the notice and consent requirements when, for example, the use of information is necessary to provide a product or service requested by a customer, protect against fraud or other liability, or comply with applicable laws.⁹

As this example suggests, notice and choice statutes often provide consumers with few meaningful choices. Gramm-Leach-Bliley, in fact, allows for just one: consumers can opt out of some, but not all, transfers of personal information to third parties for marketing purposes. As a practical matter, therefore, consumers’ only serious choice in response to the legally required notices is to choose to take their business elsewhere, assuming there is another financial institution that discloses preferable data processing practices.

But we still get notices—lots of them. In fact, then-FTC Chairman Timothy Muris commented at the end of 2001:

The recent experience with Gramm-Leach-Bliley privacy notices should give everyone pause about whether we know enough to implement effectively broad-based legislation based on notices. Acres of trees died to produce a blizzard of barely comprehensible privacy notices. Indeed, this is a statute that only lawyers could love—until they found out it applied to them.¹⁰

The irony is that no one reads these notices, and even fewer people act on them. You can hardly blame them. Because the FTC and states attorneys general have determined to treat notices as binding contracts, the people who draft them are understandably worried about being precise and inclusive. Moreover, as data protection laws and regulations become more complex, so do the notices required by those enactments.

⁷ Gramm-Leach-Bliley Financial Services Modernization Act, 106 Pub. L. No. 102, 113 Stat. 1338 (1999).

⁸ *Id.* § 503(b).

⁹ *Id.* §§ 502(b)(2), (e).

¹⁰ Timothy J. Muris, *Protecting Consumers’ Privacy: 2002 and Beyond*, Privacy 2001 Conference, Oct. 4, 2001.

The European experience has tended to go the other direction but has proved no more successful. Notices under European data protection laws are often reduced to mere warnings. One popular privacy notice throughout London and other European capitals is “Warning: CCTV in use.” These signs may motivate good behavior, but they do little to empower individuals to make informed choices about the collection and use of data about them. Similarly, many European businesses provide brief privacy notices, often of obvious data collection practices (e.g., “if you reply to this e-mail we will collect personal data about you”). I encountered one British theater box office that offered callers the option to opt out of hearing its privacy notice altogether.

The Cost of Choice

Choice has proved expensive. Costs include not only the expense of printing and mailing or otherwise distributing notices and consent opportunities that no one reads, but also the burden of unwanted and repetitive contacts to offer consumer choice opportunities and the opportunity costs of missed or ignored chances to exercise choice.

It is difficult to believe that those costs are justified. This is especially true when the choice is merely an illusion. For example, if consent is required as a condition for opening an account or obtaining a service, a high response rate can always be obtained. A useful example are the license terms that computer users encounter when downloading or installing software. The first window that opens during the installation process is a notice of terms and conditions, usually relating to intellectual property rights. The user is given two options “I Accept” or “I Decline.” Because the installation stalls until the individual makes a choice, it is not difficult to get him or her to make that choice. Moreover, because clicking on the “I Decline” button will terminate the installation process, it is not difficult to prompt the user to choose “I Accept.” Software manufacturers could accurately claim a 100 percent consent rate to their license terms, but only because consent is a condition of service.

Institutions confronted with explicit consent laws report similar results. For example, one of the United States’ largest financial institutions has reported that it has no difficulty complying with consent requirements in European countries, because it prints the opt-in notice in the account-opening form above the signature line. A consumer cannot open an account without granting consent.

The Benefits of No Choice

But the strongest indictment of the privacy-as-control model is that there are many situations in which the reliance on choice is simply undesirable. This is true of the many valuable uses of personal information where the benefit is derived from the fact that the consumer has not had control over the information. For example, credit information: its value derives from the fact that the information is obtained routinely, over time, from sources other than the consumer. Allowing the consumer to block use of unfavorable information would

make the credit report useless. In the words of former FTC Chairman Muris: the credit reporting system “works because, without anybody’s consent, very sensitive information about a person’s credit history is given to the credit reporting agencies. If consent were required, and consumers could decide—on a creditor-by-creditor basis—whether they wanted their information reported, the system would collapse.”¹¹

This helps to explain why even privacy laws that promise consumer choice inevitably remove many, if not most, uses of information from the realm over which individuals can exercise control. In the United States this is true of financial information, health information, education records, electronic communications, and the list goes on. But it is also true of the EU data protection directive and other privacy laws. In the words of Professor Schwartz: these laws “promise too much, namely data control, and deliver too little.”¹²

The Health Information Context

As important as these issues are in the context of bank accounts and direct marketing, they are especially acute when applied to health information. And the phrase “autonomy trap” is especially apt in describing them.

Autonomy in Health Care

Individual autonomy—which experts describe as “signif[y]ing control of decision-making and other activity by the individual”¹³—lies at the heart of modern health care and health law, especially in the United States. This has not always been the case, it is not the case in all countries, and as we move increasingly to a system in which health care is not only paid for by third parties, but actually managed by them as well, it is not at all clear that it will continue to be the case here. But for the moment, autonomy is the bedrock of medical practice and research. As Justice Benjamin Cardozo famously asserted in 1914: “Every human being of adult years and sound mind has a right to determine what shall be done with his own body.”¹⁴

The obvious corollary of autonomy is informed consent: If individuals have the right to control what is done with their bodies, they must certainly have the right to be told what the options are and the potential risks and benefits of each. “Informed consent is . . . a core concept central to American beliefs about individual rights and the proper relationship between patients and providers.”¹⁵ Under U.S. law today, health care providers have a legal duty to disclose to patients material information about:

¹¹ Muris, *supra* note 85.

¹² Paul M. Schwartz, “Privacy and Democracy in Cyberspace,” 52 *Vanderbilt Law Review* 1607, 1677 (1999).

¹³ Bart J. Collopy, “Autonomy in Long Term Care: Some Crucial Distinctions,” 28 *Gerontologist* 10 (1988 Supp.).

¹⁴ *Schloendorff v. Society of New York Hospital*, 105 N.E. 92 (N.Y. 1914).

¹⁵ Theodore R. LeBlang, et al, “Informed Consent to Medical and Surgical Treatment,” in *Legal Medicine* 343, 349 (S. Sandy Sanbar ed., 6th ed. 2004).

diagnosis or nature of the problem; nature and purposes (that is, expected benefits) of the proposed intervention; reasonably foreseeable risks associated with the intervention, and specifically their likelihood of happening and potential severity if they do materialize; reasonable alternatives and their benefits and risks; and the probable risks and benefits of not undergoing the proposed intervention.¹⁶

Autonomy in Health Information

Autonomy has become a foundational principle not only for health care, but for protecting the privacy of health information as well. Autonomy's essential corollary—informed consent—has made the transfer too. So in addition to the already powerful, global predilection for understanding privacy as control, with its reliance on notice and choice, we now add the additional weight of autonomy, and its reliance on informed consent. The pressure for using law to impose notice and choice requirements becomes irresistible and the recipe for disaster complete.

That confluence of forces found its highest expression to date in the health privacy rules issued in 2001 under the Health Insurance Portability and Accountability Act.¹⁷ As amended in 2002,¹⁸ the rules regulate the use of information that identifies, or reasonably could be used to identify, an individual, and that relates to physical or mental health, the provision of health care to an individual, or payment for health care.¹⁹

A covered entity may use personal health information to provide, or obtain payment for, health care only after first providing the patient with notice and making a good faith effort to obtain an “acknowledgment.”²⁰ (This is an improvement; the original rules required consent.) Notices must meet detailed requirements set forth in the rules; proof of providing notice and acknowledgments must be retained for six years after the date on which service is last provided.²¹

A covered entity may use personal health information for most purposes other than treatment or payment only with an individual's opt-in “authorization.”²² An “authorization” must be an independent document that specifically identifies the information to be used or disclosed, the purposes of the use or disclosure, the person or entity to whom a disclosure may

¹⁶ Marshall B. Kapp, “Patient Autonomy in the Age of Consumer-Driven Health Care: Informed Consent and Informed Choice,” 28 *Journal of Legal Medicine* 91, 97 (2007).

¹⁷ Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (2000) (HHS, final rule) (codified at 45 C.F.R. pt. 160, §§ 164.502, 164.506).

¹⁸ Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 43,181 (2002) (HHS, final rule) (codified at 45 C.F.R. pt. 160, §§ 164.502, 164.506).

¹⁹ 45 C.F.R. § 164.504.

²⁰ 45 C.F.R. § 164.506(a).

²¹ *Id.* § 164.105(c)(2).

²² *Id.* § 164.508(a)(1).

be made, and other information.²³ A covered entity may not require an individual to sign an authorization as a condition of receiving treatment or participating in a health plan.²⁴

A covered entity may use or disclose personal health information for directories if the covered entity obtains the “agreement” of the individual.²⁵ An agreement need not be written, provided that the individual is informed in advance of the use and has the opportunity to opt out of any disclosure.²⁶

The health privacy rules mark the apex in U.S. law of choice-based privacy law and the growing complexity of notice and consent requirements. One rule to deal with one type of information requires three different types of notice and consent. Not surprisingly, in practice, the rules have been problematic.

Health care providers are generating billions of complex privacy notices that no one is reading. I sat in one waiting room recently and watched while a receptionist handed patient after patient the mandated HIPAA disclosures with her left hand and collected them back with her right hand as patients searched for a trash can in which to discard them.

But the inadequacies of the HIPAA privacy rules are measured not only in wasteful bureaucracy and paperwork, but also in an acute awareness that the notices and choice provisions do little to enhance the protection of privacy. Moreover, the notice and choice requirements don’t apply in many settings where individuals might be thought to have the greatest interest in privacy—namely, disclosures to government officials.²⁷

But my core concern about our approach to health privacy—and this is true in other countries as well—is not the cost, inefficiency, or inadequacy of the protection, but rather its impact on health care.

The Impact on Health Care

Health care today is increasingly information driven. It was this realization that was much of the impetus behind the passage of HIPAA—to provide for the digitization and standardization of health records necessary to enhance efficiency, accountability, and transferability of those records. In the decade since HIPAA was passed, however, personal information has assumed even greater importance in health research and treatment. For example, a growing volume of research no longer involves experimenting on patients and research subjects, but rather reviewing data about actual experience with treatments and drug therapies to detect harmful side-effects, understand better the operation of medicines, develop new ones, and spot unanticipated benefits and uses for drug therapies.

²³ *Id.* § 164.508(c).

²⁴ *Id.* § 164.508(a)(2)(iv).

²⁵ *Id.* § 164.510.

²⁶ *Id.*

²⁷ *Id.* § 164.512.

Consider the treatment of diabetic retinopathy—the leading cause of blindness in the United States. One of the most widely used, and least expensive, drugs used today to shrink the size and slow the growth of blood vessels that unchecked will blot out vision is Avastin. Originally used to slow the growth of cancer in the colon, researchers discovered that one beneficial side-effect of this drug was to do the same in the eye. They learned this by examining tens of thousands of records on patients to find enough patients with both colon cancer and diabetic retinopathy to make it possible to document the side-effect.

As this example suggests, not only is patient data a critical resource for research, but it is also essential to finding appropriate research subjects. For example, when Eli Lilly was developing inhalable insulin, one potential concern was how the therapy would be tolerated by people with asthma or chronic obstructive pulmonary disease. Conducting the research necessary to answering those questions required locating insulin-dependent diabetics with asthma or copd who are not on inhaler therapy —no mean feat—and in the case of copd, diabetics who had never smoked—a near-impossibility since smoking is the leading cause of copd. Access to patient records was critical to accomplishing this. And the inability to identify and locate appropriate research is a significant contributor to delaying the approval of new drugs.

Access to information is essential to pharmacovigilance and post-market surveillance—determining harmful side effects or interactions of drugs.

Hospitals and medical centers digitize and centralize patient records to increase efficiency, save money, enhance accountability, decrease the burden on individuals and institutions of duplicative paperwork, and, most importantly, to provide a broader picture of each patient necessary to enhance the speed and accuracy of diagnoses and reduce medical inaccuracies and avoid harmful drug interactions. These are all critical goals that require broad access to records throughout the system. In addition, there are important, valuable uses for those data that require access to all patient records—whether evaluating the effectiveness of treatment protocols, checking for physician overprescribing or misprescribing, and improving the quality and efficiency of service provided by the institution.

I could go on, but I hope I don't need to convince you that access to personal data is essential for medical research and treatment. But this will only become more true in the future. All of the talk in health care today is about “personalized medicine.” This is the new mantra at the NIH, the FDA, and HHS. This term means many things, but almost all require access to personal data.

Mike Leavitt, Secretary of Health and Human Services, identified personalized medicine as one of his key objectives and outlined the need for personal information in a series of speeches beginning last year:

The next ten years will be seen as a signal point of transition in healthcare. Medicine will be transformed from an instinctive art of alleviating symptoms to a science of personalized health care.

The next several years will be viewed by future generations as the time when treatments became preventive, predictive, and personalized.

This transformation will touch every aspect of care—from sensors that allow doctors to detect the first sign of cancer to information networks that allow scientists to scan hundreds of thousands of records for the scent of a cure to a debilitating disease.

A decade from now, we will have a health care delivery system in which doctors, pharmacists, and other health care providers customize treatment and management plans for individual patients based on vast amounts of information that is readily accessible at clinics and hospital bedsides—information like medical history, genetic variability, and even patient preferences. . . .²⁸

While not all of the features of the bright future about which Secretary Leavitt speaks so glowingly may materialize any time soon, it is indisputable that health care research is moving towards greater targeting of drug therapies. Pharmacogenomics—the science of tailoring drug therapies to specific genetic make-ups—is a major and growing focus of the FDA, pharmaceutical companies, and medical researchers. The goal is to create drugs, determine dosage and therapies, and prevent harmful—even life-threatening—reactions all based on human genotype.

It sounds very futuristic, but it is happening already. In fact, earlier this month the FDA approved its first drug labeling requirement that specifically includes a warning for people with a specific genotype. The drug is the blood thinner Coumadin (warfarin) , and while it is a lifesaver for tens of millions of people who take it to prevent blood clots, heart attacks, and strokes, for about one-third of patients with a distinct variation of two genes, the drug can cause life-threatening internal bleeding. In fact, it is the second most common drug—after insulin—implicated in visits to emergency rooms for adverse drug events. The new labeling requirement warns patients and physicians about this genetic sensitivity. According to FDA Commissioner Andrew von Eschenbach, MD, it is “is one step in our commitment to personalized medicine. . . [to] using modern science to get the right drug in the right dose for the right patient”²⁹

Many of our treatments that save the lives of many, but kill a few. Genetic research is already helping us identify those at risk so that they can receive alternative treatments. For example, “[p]atients with two copies of the gene for an abnormal clotting factor face a risk of

²⁸ Remarks of the Hon. Mike Leavitt, Secretary of Health and Human Services, to the BIO Annual Convention, April 11, 2006.

²⁹ “FDA Updates Labeling for Blood-thinners Coumadin and Warfarin,” *Medical Device Week*, Aug. 20, 2007.

developing blood clots in the leg that is 50-100 times greater than that of the general population. [Physicians] can use this information today to improve the quality of care for patients who may be immobilized for a substantial period, such as following major orthopedic surgery.”³⁰

Jonathan B. Perlin, Undersecretary of the Department of Veterans Affairs, testified before Congress last summer that “[g]enetic analysis is becoming part of standard care for treatment of many cancers, including most leukemias and lymphomas, brain tumors, colon cancer and breast cancer. These analyses are used both to diagnose the disease and to determine responsiveness to both chemotherapy and radiation. Cancer screening based on molecular genetic and proteomic tests will help to catch disease earlier, enabling cures for patients who now go one to develop metastases and die.”³¹

Secretary Perlin stressed the importance of investing in “the achievable possibilities of genetic medicine to understand the role of genetics in the prevention and cause of disease; to improve how clinicians prescribe medications; to prevent adverse drug reactions; and to learn how to use genetic information effectively in everyday practice.”³²

The Problem of Privacy Law

But you can see the problem of genetic research and treatment therapies that focus on smaller and smaller subsets of the population. Access to large amounts of personal data is essential to identify genetic patterns. Access is also necessary to identify and recruit research subjects that meet ever more specific and hard-to-satisfy criteria. And access is necessary to determine who should receive a genotype-based therapy. In fact, the volume of data required for most research is becoming necessarily global.

How does privacy law stack up against the current and changing demand for data? Not well. Under HIPAA, research can be conducted using patient data primarily only if one of four conditions are met.

The first is using deidentified data. This requires removing 18 data elements, including not only obvious information, such as name and contact information, but also all geographic subdivisions smaller than a state (except for the initial three digits of a ZIP Code in certain limited circumstances), all date elements except year, and any biometric identifiers.³³ This provision is useless for medical research of almost any form.³⁴ How can one do genetic research if the record can’t include genetic information, which is by definition a biometric identifier?

³⁰ VA Medical and Prosthetic Research, Hearing before the Comm. On Veterans Affairs, House of Representatives, June 7, 2006 (testimony of Jonathan B. Perlin, Undersecretary of the Department of Veterans Affairs).

³¹ *Id.*

³² *Id.*

³³ 45 C.F.R. § 164.514(b)(2)(i).

³⁴ See David Casarett, et al, “Bioethical Issues in Pharmacoepidemiologic Research,” *Pharmacoepidemiology* (R.L. Strom ed., 4th ed., 2005), at 595.

How can one examine drug interaction if the relevant date information has been reduced to the year?

The second alternative under HIPAA allows researchers to obtain access to a “limited data set” that has 16 of the 18 data elements required for true de-identification removed, if the researchers have executed a “data use agreement.” A limited data set may not include biometric identifiers, and so, while it may be useful for some types of medical research, it will not suffice for genetic research.

The other two alternatives both involve consent. One way to satisfy HIPAA’s requirements is to obtain the informed consent of the data subject. The other way is to get the approval of an Institutional Review Board. Neither way has proved an efficient or reliable way of conducting research.

Obtaining individual consent is often problematic for many reasons. The number of people from whom consent is needed is large, especially as research hones in on diseases and therapies affecting fewer and fewer people. Consent is easiest to obtain at time of admission to a hospital or when treatment is begun, but it is often impossible to anticipate all of the uses to which data may be put so far in advance. As a result, consent can degenerate into a request for blanket approval for any use of personal data, thus making a mockery of the requirement and satisfying neither the spirit nor the letter of the law affecting informed consent. Moreover, the person or entity managing the admission or treatment is rarely the same one as will conduct the research, so obtaining consent in advance requires one institution obtaining consent for the research of another. Also, at time of admission to a hospital or the beginning of a treatment relationship, patients are often focused on their immediate health care and not particularly interested in addressing matters concerning the prospective future use of their health information.

Obtaining consent at a later date is even more problematic. The patient must still be living, which is often not the case, especially when research involves life-threatening conditions. The patient must be located. With 42 million Americans moving every year, this is easier said than done. Then they have to be contacted, which is both expensive and time-consuming. Then of course they have to consent. This is all necessary just to obtain their permission to examine their medical records. When searching for a research subject with a particular genetic make-up or the insulin-dependent diabetic with asthma, hundreds or even thousands of records have to be examined just to find one person who can then be asked to participate in a research study.³⁵

As world-renowned bioethicist Arthur Caplan and his colleagues have noted:

[I]f individuals must be contacted every time their records may be used in a particular study, the individual may consider such contact intrusive. Furthermore, individuals might consider that their confidentiality has been

³⁵ See U.S. General Accounting Office, *Medical Records Privacy* (GAO/HEHS-99-55), at 14-15 (1999).

violated if researchers access research information and contact them directly in order to obtain consent for the use of de-identified records. Individuals may refuse participation if contacted for a study they consider irrelevant to their health. An individual may also become alarmed if asked to consent for records to be used in such a study of a disease for which she has not been diagnosed. . . .³⁶

The requirement for patient consent for medical data to be examined poses a practical and serious impediment to epidemiological research. A 1999 study, enacted before the HIPAA rule took effect and therefore able to compare participation rates in research studies in states with different consent requirements, found that in states where research access to medical records did not require patient authorization, investigators were able to access 93% of the potential study population. But in states where consent was required, only 19% of the available population participated.³⁷

Some large medical institutions with extensive treatment and research programs, such as the Mayo system, have proved successful in obtaining a high rate of consent. But even there, the 20% of people who refuse to consent or to make a decision of any form exhibit distinct demographic and health characteristics that are statistically capable of skewing the research base. Dr. Caplan and his colleagues noted that even when the refusal rate was as low as 3.2%, “the persons declining consent varied from the study population by age, gender, residence, and prior diagnoses, suggesting that the ability to opt out of databases creates a potential bias in the data.”³⁸

The IRB approach is the one most often relied on, but its success depends on finding a cooperative committee that is not too meticulous in its reading of the law. What the HIPAA privacy rule actually requires is that an IRB may substitute its consent for that of the data subject only if three conditions are met. Two are relatively easy to satisfy—that the “research could not practicably be conducted without the waiver or alteration” and that “the research could not practicably be conducted without access to and use of the PHI.”

The third is that the “use or disclosure of the PHI involves no more than minimal risk to the privacy of individuals.” “Minimal,” as defined by federal law, means no greater than if the subject did not participate in the research.³⁹ Given the raft of security breaches and problems with obsolete medical records being found in storage units and garbage cans, how many people in good faith could certify that research involving sensitive health information presents no greater risk to the data subjects than if their data had not been used?

The real difficulty for IRBs is that they are charged by law with two primary tasks: balancing the potential benefits of proposed research with the risk to the research subject and

³⁶ David Casarett, et al, at 593.

³⁷ D.B. McCarthy, et al, “Medical Records and Privacy: Empirical Effects of Legislation,” 34 HSR: Health Services Research 417 (1999).

³⁸ David Casarett, et al, *supra* at 594.

³⁹ 45 C.F.R. § 46.102i.

ensuring that the researchers obtain the informed consent of the research subjects to appropriate research. Their members bring their diverse and professional judgment to ensuring both that the benefits and risks are adequately described to the research subject and that the request being made to the data subject is objectively reasonable. Unlike most privacy laws, under the federal government's Common Rule, which applies to all federally funded research involving human subjects, consent is only an answer if the question being asked is reasonable.⁴⁰ Yet as Dr. Caplan and his colleagues have noted, "[t]he risks to the subjects of epidemiology research are not the usual health risks of research that can be balanced against the potential health benefits of research. They are largely risks of another kind."⁴¹ And risks that IRBs are neither familiar nor experienced with resolving.

Moreover, IRBs live in a world of autonomy and informed consent. Providing an adequate disclosure and obtaining meaningful informed consent is the foundational principle of almost all research that involves human subjects. In situations where consent is impossible, for example, studies involving deception, IRBs often raise serious concerns and require substantive post-research debriefing of the research subjects, among other ameliorative measures. Asking an IRB to substitute its judgment for that of the data subject is contrary to its basic mandate and mode of operating.

These are just the basic consent requirements of HIPAA. There are, of course, others that apply even to research, and many more that apply to the use of personal information for treatment. Moreover, despite the growing nationalization and even globalization of health research, HIPAA's drafters allowed individual states to adopt more onerous requirements, which a number have done. And, of course, other nation's laws, such as those adopted under the EU data protection directive, are usually more restrictive still.

Three Conclusions

I am left with three conclusions. The first, is that for both practical and ethical reasons we need to move away from requiring individual patient consent before medical records are examined for research purposes. For too long we have failed to recognize the important distinction between privacy of the body—the right to refuse treatment or to choose among medically appropriate treatments—and privacy of information *about* the body.

Helena Gail Rubinstein, a former Director of Policy Analysis and Program Development in the Massachusetts Group Insurance Commission, has written that "while autonomy is an appropriate framework for evaluating questions concerning the treatment of one's body, it is not the appropriate framework for evaluating rules to regulate the use of health data."⁴²

⁴⁰ 45 C.F.R pt. 46.

⁴¹ *Id.* at 597.

⁴² Helena Gail Rubinstein, "If I Am Only for Myself, What Am I? A Communitarian Look at the Privacy Stalemate," 25 *American Journal of Law and Medicine* 203, 223 (1999).

Of course there need to be requirements for appropriate safeguards in place so that data intended for research is protected from accidental or deliberate reuse or misuse. I would also require that visibly identifying information, such as name, phone number, and Social Security Number be removed or blocked out on records shared for research purposes. These and other appropriate requirements can be overseen by institutional data stewards and IRBs, as they have been for decades. But I would no longer condition access to reasonably anonymized medical data on individual consent.

This position can be justified on practical grounds: the difficulty and, in many cases, impossibility of obtaining consent, the burden to individual patients of being bombarded with consent requests, the time and money wasted by complying with and overseeing the bureaucracy we have built up around consent requirements, and by the fact that we have largely reduced consent to an all-or-nothing paperwork requirement that provides individuals with little meaningful opportunity for choice anyway. Think for a moment about the informed consent process we use in other settings, such as medical treatment. We admit someone to a hospital, begin the process of anesthetizing them, and then shove a 25-page informed consent form under their noses and tell them to sign. Then we feel good that we have gotten their full, informed, and voluntary consent.

But I think moving away from conditioning the use of medical information for research on consent is justified on ethical grounds as well. As Ms. Rubinstein writes: relying on consent refuses to recognize “in exchange for the vast improvements in medical care, a correlative responsibility on the part of the individual, as a potential consumer of health care services, toward the community. As individuals rely on their right to be let alone, they shift the burden for providing the data needed to advance medical and health policy information. Their individualist vision threatens the entire community. . . .”⁴³

We have already eliminated the requirement of consent in other areas in which society—or the Department of Health and Human Services—believes that the social utility of the information outweighs the privacy interest. Non-consensual disclosures of health information are permitted for public health activities; to report victims of abuse, neglect, or domestic violence; in judicial and administrative proceedings with a court order, subpoena, or discovery request; to enable product recalls, repairs, or replacement; to facilitate organ and tissue transplantation; for law enforcement activities with a warrant, a subpoena, an administrative request, an investigative demand, or even a law enforcement official’s request.⁴⁴ And in these settings, there are no meaningful limits on subsequent use, no anonymization requirements, no security standards, and no provisions for oversight.

In the case of health research and health care, the development and targeting of new therapies, speeding up approvals for new drugs, avoiding harmful and life-threatening reactions to treatment, enhancing accountability in health care delivery, and improving its efficiency all depend

⁴³ Id. at 226.

⁴⁴ 45 C.F.R. § 164.512.

on ready access to reliable personal information. The need is clear, the benefits have already been demonstrated to be enormous, and the potential for the future is vast.

These issues are being raised by medical professionals, ethicists, patient groups, researchers, and government officials. Some other legal systems have begun to grapple successfully with them. Ontario, for example, has adopted a health privacy law that allows researchers unfettered access to personal health information for research, once the provincial Information and Privacy Commissioner—Dr. Ann Cavoukian—has certified the researchers to be prescribed entities that meet important rules that limit reuse and ensure that the data are protected. This is an important model that other jurisdictions would do well to examine closely.

My second conclusion is that for the public and the political powers to tolerate the intensive use of personal information that is inescapable to support medical research and personalized medicine, we are going to have to create stronger, more substantive tools for protecting privacy. The one point on which everyone in the medical community seems to agree is that public trust is critical. That trust is built on the public's confidence that their information is being used appropriately, for worthwhile ends, and subject to meaningful protection. As Secretary Leavitt has stressed:

One of the most pressing questions for the transition to personalized medicine is privacy. People worry that confidential personal information will be misused.

The reality is, if they are not fully confident of the security of their data, people will not participate. It is as simple as that.

It will not be the technology or the science that limits progress. It will be sociology.

. . . . Our regulatory system is not yet prepared to deal with it. We have to reinvent the regulatory process so we are enabling, not inhibiting, progress and we will.⁴⁵

I believe this requires not only the types of provisions I have just outlined, but also serious federal governmental oversight and meaningful enforcement. It also requires a culture among medical institutions and the research community of greater responsibility and accountability for the collection, storage, and use of personal data.

Finally, while the reliance on autonomy as a basis for regulating personal data is especially misplaced, and the need for more substantive and rational protections for personal data especially acute, in the context of medical research and therapy, I believe these critiques also apply in other contexts. In the face of widely distributed, affordable digital technologies and a world in which almost every activity is becoming increasingly information-dependent,

⁴⁵ Leavitt, *supra* at 4.

privacy-as-control is often no longer realistic, appropriate, or desirable. It creates an impossible burden for individuals to say “you exercise control over your own data.” Increasingly, it cannot be done, we know it, and it is high time we admit it and begin searching for better, more substantive protections for personal privacy instead.