Protecting Patient Privacy:

STRATEGIES FOR REGULATING ELECTRONIC HEALTH RECORDS EXCHANGE

NYCLU
NEW YORK CIVIL LIBERTIES UNION

NEW YORK CIVIL LIBERTIES UNION

125 Broad Street, 19th Floor
New York, NY 10004
www.nyclu.org

March 2012

ACKNOWLEDGEMENTS

This paper was written by Corinne A. Carey, NYCLU assistant legislative director, and Gillian Stern, volunteer attorney with the NYCLU. Research assistance was provided by Erika Rickard and Andrew Napier. Special thanks to outside readers Gretl Rassmussen and Jeanne Flavin.

It was edited by Robert Perry, Jennifer Carnig, Melissa Goodman and Helen Zelon.

Graphics were created by Willa Tracosis.

It was designed by Li Wah Lai.

ABOUT THE NEW YORK CIVIL LIBERTIES UNION

The New York Civil Liberties Union (NYCLU) is one of the nation's foremost defenders of civil liberties and civil rights. Founded in 1951 as the New York affiliate of the American Civil Liberties Union, we are a not-for-profit, nonpartisan organization with eight chapters and regional offices and nearly 50,000 members across the state. Our mission is to defend and promote the fundamental principles and values embodied in the Bill of Rights, the U.S. Constitution, and the New York Constitution, including freedom of speech and religion, and the right to privacy, equality and due process of law for all New Yorkers. For more information about the NYCLU, please visit www.nyclu.org.

Protecting Patient Privacy: STRATEGIES FOR REGULATING ELECTRONIC HEALTH RECORDS EXCHANGE

CONTENTS

GLOSSARY OF TERMS

BREAK THE GLASS. A provision in New York State's policies and procedures that refers to the ability of a health care provider or other authorized user to access a patient's Protected Health Information (PHI) without obtaining patient consent. NYS policies allow a provider to "break the glass" in the case of a medical emergency where a patient is unable to give consent to access his or her health information.

COVERED ENTITY. Those entities that are required to comply with federal health information privacy rules under HIPAA, which defines a "covered entity" as (1) a health plan, (2) a health care clearinghouse, or (3) a health care provider who transmits any health information in electronic form for insurance or reimbursement purposes.

DATA MINING. A process of pulling pieces of data from a database or electronic network in order to look for patterns and relationships. In the context of health information technology, data mining can be used for public health purposes, for example, to identify patterns that reveal an epidemic. But it can also be used for marketing purposes to determine where to focus promotional campaigns.

DATA SEGREGATION/GRANULAR CONTROL. The ability to separate out or sequester health information, sometimes based on specially protected sensitive health information but not always. Data segregation or granular control 1) allows patients to exert some control over the type and level of information that can be shared; 2) restricts information access to specific individuals or entities; and 3) establishes preferences for time frame and/or duration during which specific information can be electronically accessed.

EHR (*Electronic Health Record*). A digital version of the traditional paper-based medical record for an individual either kept within a single facility, such as a doctor's office or a clinic (sometimes referred to as an electronic medical record or EMR), or the official health record for an individual that is shared among providers, facilities and agencies.

HEAL-NY. New York State passed the *Health Care Efficiency and Affordability Law for New Yorkers* Capital Grant Program in 2004, often referred to as the HEAL NY Program, to support the development and implementation of New York's health information technology infrastructure.

HIE (*Health Information Exchange*). Generic term for any system that facilitates electronic exchange of medical information. Alternatively, HIE refers to the act of transmitting or exchanging electronic medical information among facilities, health information organizations (HIOs) or HIEs, and government agencies.

HIO (*Health Information Organization*). An entity that facilitates electronic exchange of medical information. A HIO is one type of HIE; for example, a RHIO, or Regional Health Information Organization, is an HIE.

HIPAA. *The Health Insurance Portability and Accountability Act* (HIPAA) was enacted by Congress is 1996. The HIPAA Privacy Rule (45 CFR Part 160 and Subparts A and E of Part 164) regulates the use and disclosure of personal

health information (or Protected Health Information) held by "covered entities."

HIT (*Health Information Technology*). The storage, retrieval, exchange and use of health information in an electronic environment.

HITECH. Enacted as part of the American Recovery and Reinvestment Act of 2009, the *Health Information Technology for Economic and Clinical Health* (HITECH) Act is designed to promote the widespread adoption and standardization of health information technology. HITECH required the Department of Health and Human Services (HHS) to amend the HIPAA Privacy, Security, and Enforcement Rules to strengthen privacy and security protections for electronic health information sharing.

IT (*Information Technology*). The development, implementation, and maintenance of computer hardware and software systems to organize and communicate information electronically.

NCVHS. The *National Committee on Vital and Health Statistics* (NCVHS) was established by Congress to serve as an advisory body to the Department of Health and Human Services on health data, statistics and national health information policy.

NwHIN. The *Nationwide Health Information Network* (NwHIN) is sometimes described as a "network of networks" that allows participants (state level exchanges, federal entities, public health entities and health information organizations) to locate and exchange health information electronically. The initiative is sponsored by the Office of the National Coordinator (ONC) for Health Information Technology, which began developing the NwHIN in 2004.

NYeC (The *New York eHealth Collaborative*). A state designated not-for-profit public-private partnership and statewide policy body formed in 2006 that is charged with the development of policies and procedures governing the implementation of the electronic exchange of health information in New York State.

OHITT. New York State's *Office of Health Information Technology Transformation* (OHITT) was created in 2007 by the New York State Department of Health to coordinate New York's Health Information Technology efforts.

PHI (*Protected Health Information*). PHI is defined by HIPPA (federal law) as any information held by a covered entity that concerns health status, provision of health care, or payment for health care that can be linked to an individual. This is interpreted rather broadly and includes any part of an individual's medical record or payment history.

PHR (*Personal Health Record*). An electronic health record maintained by a patient that includes, for example, patient-reported data, as well as physician-generated data and lab results (either entered by the patient or downloaded from the lab itself). A PHR differs from an EHR, which is maintained by provider or a health information exchange.

RHIO (*Regional Health Information Organization*). A group of organizations within a specific geographical area that share health care-related information electronically. A RHIO typically oversees the means of information exchange and develops health information technology (HIT) standards.

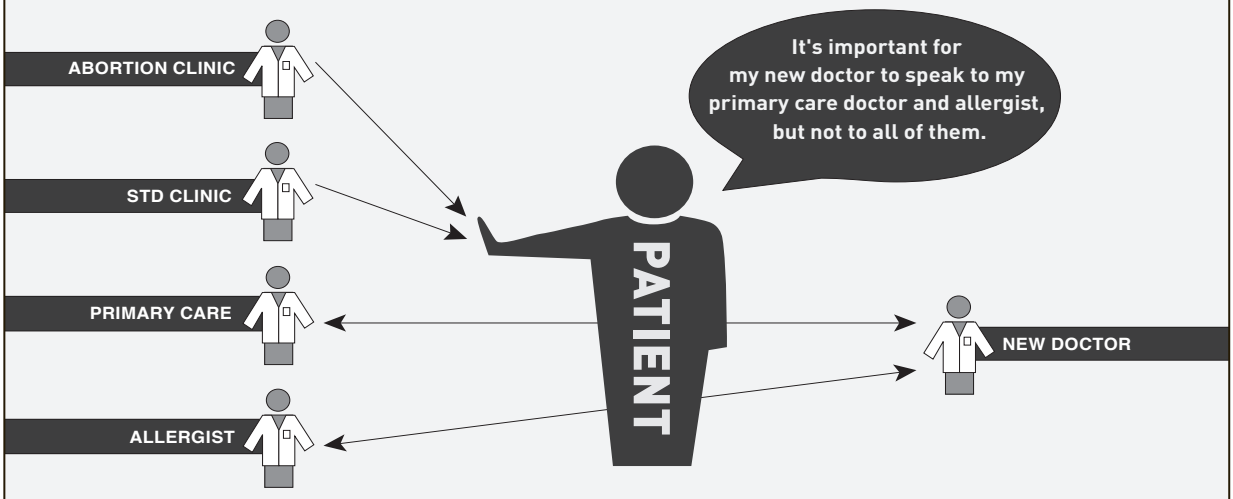
SHIN-NY (*Statewide Health Information Network for New York*). Described as an "information superhighway," the SHIN-NY is the technological infrastructure being designed by New York to facilitate the exchange of health information between and among providers, consumers, payers and government agencies.

PROTECTING PATIENT PRIVACY

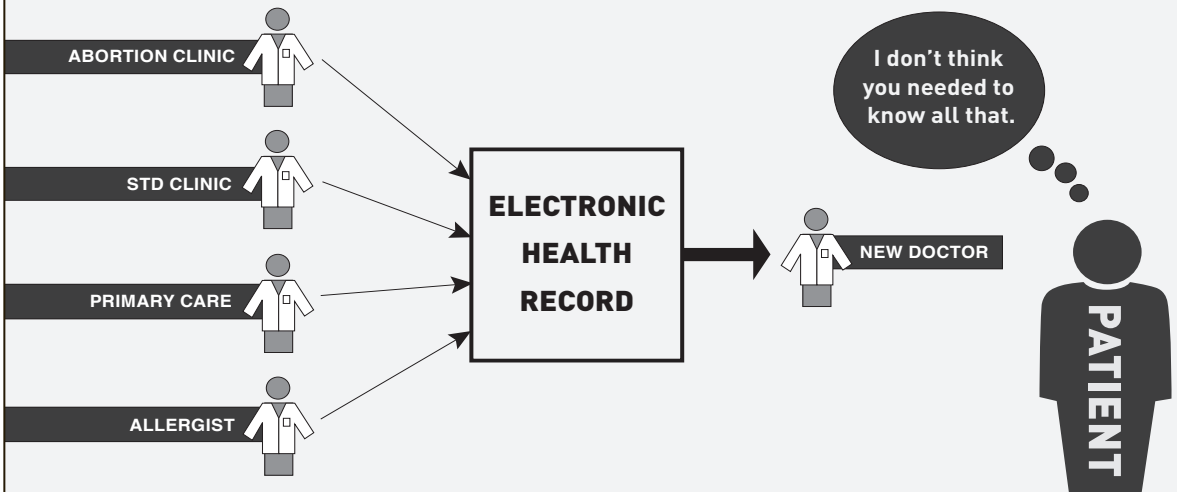
Who gets to see your medical history?

Until the advent of electronic health information exchange, patients had the ability to control which providers had access to what information about their medical history. Even when a patient consented to allow a new provider to access her records, what information went into those records depended on what the patient wanted to tell her doctor, and then what the doctor chose to send to the new provider. Unless exchange networks are carefully designed, electronic health records that can be shared at the click of a mouse can threaten patient control over sensitive health information.

Traditional patient privacy controls



Patient privacy in an electronic world



INTRODUCTION

Electronic health information technology is transforming the health care system as we know it. Like many aspects of our lives, the medical office is going online. Doctors, health systems, insurers, care coordination systems, regulators, governments and patients themselves are demanding electronic access to health records. Near instantaneous sharing of information between and among health care providers promises significant benefits to both doctors and patients, including greater coordination and efficiency in service delivery, reductions in medical errors and misdiagnoses, and convenience. These benefits are also likely to improve the efficiency and effectiveness of the health care system more broadly.

However, this step forward poses significant risks. Easily shareable electronic records threaten patient privacy, and can lead to security breaches, misuse of information, and most importantly, loss of patient control over confidential and sensitive health information. This threatens the confidential communication between doctors and patients that has been a bedrock principle of modern medicine. Confidentiality ensures that patients seek out care, and that they are open and honest with their providers. Fully informed by the totality of a patient's circumstances, providers can render the best care possible.[1] Patients who fear a loss of control over their private medical information may lose faith in their doctor—and in the health care system. They may fail to share critical information with their treating providers or they may avoid treatment altogether.

Guaranteeing confidentiality and patient control over sensitive health information is critical to the success of electronic health information exchange. Only with confidence that personal medical information will be shared in ways that benefit them and not cause them harm will patients fully engage in this promising technological advancement.

New York State has taken a national leadership role in transforming the manner in which patients' records are created and shared. Hard-copy documents and electronic records stored in an office computer are now being converted into a comprehensive, statewide network of integrated, searchable databases—with the goal of ultimately linking to a future nationwide health information network.

A growing information-sharing network, guided by the New York eHealth Collaborative, a public-private partnership funded by the New York State Department of Health, has invested more than $840 million towards developing health information exchanges, or HIEs. A dozen existing HIE networks will eventually permit providers and payers to gain access to a patient's aggregated medical records in New York State and, ultimately, connect New York's HIEs with a national network.

The state has endorsed a set of privacy and security policies and procedures for the implementation of health information exchange.[2] But these policies have significant flaws that pose challenges to the integrity of electronic record-sharing in New York State. Most significantly, these policies do not allow for patient control over the inclusion of their health information in the network. In addition, the technological infrastructure used by the state's HIEs represents an all-or-nothing approach: Once a patient consents to allowing a provider to gain access to his or her medical records, the provider sees everything that was ever entered into the network about that patient, regardless of whether the information is relevant to current treatment.

The New York Civil Liberties Union supports electronic sharing of medical records, but takes the position that patients must be able to control who has access to their medical information. Patients must also be assured that those who do have access receive only information that is relevant to their treatment. Otherwise, those in need of medical care may be reluctant to seek it or to give providers consent to review their medical records. Patients will have confidence in the state's approach to electronic health information exchange where ***vigorous informed consent*** requirements and specific ***limitations on information-sharing*** protect sensitive information and ensure individual control of personal medical records.

The New York State Department of Health, the NYeHealth Collaborative, and the New York State Legislature must take steps to protect individual privacy and autonomy as the state develops a centralized electronic exchange of health and medical information. The NYCLU offers the following recommendations in support of this goal.

- **Give Patients and Providers Control Over Access to, and Sharing of, Medical Records.** Information-sharing data systems must be designed to sort and segregate medical information to comply with privacy protections guaranteed under New York State and federal laws. At present they do not. Without such protections, people who receive medical care that requires strict confidentiality—for example, treatment of conditions to which stigma attaches—and the providers who deliver that care may choose not to share medical records in order to protect privacy. This increases the risk of harm to patients and to the general public.

- **Offer Patients the Right to Opt-Out Altogether.** The state must adopt a policy that requires providers to offer patients the option of declining to participate in health information exchange altogether, or at least ensure that a patient's identifying information is not accessible by those who have not obtained the specific consent of the patient.

- **Require Patient Consent Forms to Offer Clear Information-Sharing Options.** The state must revisit its policy on consent to allow greater patient control over how medical information is shared. Consent forms should offer patients three distinct options: to opt-in and allow providers access to their electronic medical records, to opt-out except in the event of a medical emergency, or to opt-out altogether.

- **Require Notice to Patients When Their Providers Become Data Suppliers.** The state must adopt a policy mandating that providers notify patients when the provider links to an HIE. In the absence of consent to upload patient information, patients must be notified when information about them from their provider initially becomes accessible through an HIE.

- **Guarantee the Right of Patients to Correct and Amend Information.** Current law permits patients to review and submit amendments to medical records held by individual providers. The practice of correction and amendment must be adapted to ensure that a correction to any error is automatically sent to any provider who has previously accessed the patient's medical record through an HIE.

- **Prohibit, and Sanction, the Misuse of Medical Information.** The state should adopt a policy that prohibits, and strongly sanctions, the misuse of patient medical information obtained through an HIE. New York's current all-or-nothing data-sharing system gives providers access to all of a patient's medical records—regardless of how old the information or how relevant it is for current treatment. New York must protect patients from bad actors: that small minority of providers who may abuse information out of fear, prejudice or malice.

- **Mandate Redisclosure Prohibitions for Third Parties.** Current state policies do not require HIEs to warn those who access patient health information that redisclosing sensitive medical information without patient consent violates the

law. State policy should require HIEs to explicitly communicate to third parties that redisclosure is prohibited and that there are penalties for violating this prohibition.

- **Prohibit Health Information Exchanges from Selling Data.** The New York State Legislature should pass legislation prohibiting HIEs from selling patients' private health information; this prohibition should apply to records with or without a patient's personal identifiers. Medical information must not be used to target individuals or providers for promotional pitches or advertising campaigns; nor should HIEs be allowed to profit from the sales and marketing opportunities created by the release of information in patients' medical records.

- **Carefully Regulate the Use of Commercial Vendors of Personal Health Records.** A number of commercial vendors now offer patients the ability to collect, store and manage their own medical information online. State and federal confidentiality restrictions may not apply to information held by these commercial vendors. If commercially available health records systems are offered to New Yorkers as a way for them to access and manage their own health information, the state must require that patients be warned of privacy risks. Patients must also be given access to their records without having to resort to a commercial vendor.

- **Step Up Public Outreach Efforts.** Public health officials must fully inform New Yorkers about the implementation of health information exchanges (HIEs) in New York State. Under current state policy, patient medical information is linked to the system without patient notice or consent. Patients require a better understanding of what is at stake. This requires clear informed consent mechanisms and a robust public education program that explains to people what they need to know about electronic medical records exchange ***before*** a visit to the doctor's office.

PART 1: The New World of Electronic Health Information Exchange

The art of medicine faces a technological re-invention as record-keeping moves from file cabinets and desk drawers to a web of interconnected computer database systems. As cumbersome paper records are supplanted by ostensibly secure electronic networks, physicians, insurers, health care coordination systems, regulators, governments and patients themselves are eager for rapid electronic access to health records. Accordingly, New York State has begun to transform the procedures by which patient records are created, stored and shared. Hard-copy documents, once stashed in a folder or stored in an office computer, are now being converted into a comprehensive, statewide electronic network of integrated, searchable databases that will one day link to a national health information network.

Since 2004, New York State has been working to develop electronic health information exchanges (HIEs) via the New York eHealth Collaborative, a public-private partnership funded by the New York State Department of Health. In many parts of the state, shareable electronic health record systems are already up and running. Twelve regional health information organizations (RHIOs) in New York permit providers to share patient records with other providers in their networks. Eventually, all of New York's RHIOs will be linked to a statewide health information network (or SHIN-NY).[3] Other types of health information organizations will be able to access this network, and it will soon become directly accessible by individual providers.

Rapid information sharing promises significant benefits to health care providers and patients. The advent of electronic information exchange will also benefit the health care system. Services can be better coordinated and more efficiently delivered, and the incidence of medical errors and misdiagnoses can be reduced as information becomes more accessible and convenient for both patients and providers. But networked electronic records create the potential for security breaches,[4] misuse of information, and loss of patient control over confidential and sensitive health information.

Privacy protection and informed patient consent must be the foundational principles of a fair, effective electronic health information exchange. Without guarantees of privacy, shared networks will fail.[5] If private medical information is vulnerable to public dissemination and inspection, medical consumers may avoid care. And if significant numbers of patients decline to participate, the personal and public health benefits of HIE will be diminished. The potential for public backlash is great—one need look no further than the periodic public uproar over changes in Facebook's privacy practices as an example.[6] Robust and enforceable privacy protections and consent procedures must be in place from the start in order to ensure patient confidence.

What Came Before

Patient privacy has been paramount in medical care at least since Hippocrates' famous oath, which impels physicians to keep confidential any information obtained in the course of treating a patient.[7] Until very recently, patient information was kept in physical form; thus, safeguarding privacy was relatively simple. To share patient information with another provider, the doctor would secure the patient's permission, copy the relevant portion of the patient's file and send it along. Consent was required for each communication, and the patient retained the ability to control which providers had

access to what information. Even when records were shared, the information that went into those records was limited by what the patient wanted to tell the doctor; and subsequently what the doctor chose to send to another provider. A patient visiting a podiatrist might understandably choose not to disclose his prior psychotherapy, for example. When asked about past surgeries, he may share that he's had an appendectomy but omit mention of hemorrhoid surgery.

Moreover, the actual sharing of records by doctors has always involved a second screening step. Doctors and facilities rarely if ever transmit entire patient records to a second provider—they omit extraneous information, and they frequently safeguard sensitive information at the request of the patient. As in the example above, the general practitioner would inform the podiatrist of a diabetes diagnosis, but would not pass on the name, or even the existence, of the patient's psychotherapist—if the general practitioner even knew it.

Indeed, the confidentiality of individual medical records has long been mandated by professional practice standards, and by federal and state laws. All modern medical schools administer oaths that impose the duty of confidentiality on physicians.[8] Nationally, a basic right to confidentiality was codified in federal law in the Health Insurance Portability and Accountability Act (or HIPAA);[9] even stronger protections were extended by the recent American Reinvestment and Recovery Act.[10] Additional privacy safeguards protect specific categories of sensitive information like family planning services, substance abuse treatment and genetic testing.[11] Federal laws set the minimum standard; state laws frequently impose even more stringent confidentiality protections.[12] All of these patient privacy protections are rooted in the understanding that compromising patient privacy means compromising individual care and the public health.

New York State has long been a national leader in protecting the confidentiality of personal medical information. State law has strict privacy standards for medical records.[13] Unlike HIPAA, New York requires patient consent before a physician can disclose an individual's medical information to another treating physician.[14] It also limits disclosure to immediately relevant information.[15] Even stronger protections restrict the release of certain especially sensitive information regarding genetic tests,[16] mental health,[17] medical treatment of adolescents[18] sexually transmitted infections[19] and HIV.[20]

Maintaining Privacy Protections in the Face of New Technology

Advances in technology do not void existing state laws or eclipse the ethical concerns that gave rise to those laws. Rapidly evolving information technology requires that the state undertake a comprehensive in-depth analysis to determine (1) whether current policies and procedures governing HIEs comply with existing laws; and (2) whether laws protecting the confidentiality of patients' medical information are sufficient in light of new technological capabilities.

New York State laws governing personal medical information were drafted for the world of paper records; inherent in these laws is a presumption that patients control the dissemination of their medical records and that a physical "human filter" in the doctor's office decides what information is shared with third parties. Electronic systems that share entire records at the click of a mouse cannot help but undermine these controls.

Nowadays, the challenge of protecting confidentiality is exacerbated by the complexity of the modern health care system where records migrate beyond the confines of the doctor's office. Existing law has been amended to require that medical information is kept confidential not only by the doctor but by the array of other entities that have access to private medical information: HMOs, the laboratories that process medical tests, the hospital system in which the doctor participates, the doctor's or hospital's records management company, the patient's insur-

ance company, and the medical underwriter who insures that insurance company.[21]

Failing to extend the strong medical privacy protections that exist in current law to electronic health information exchange creates a serious risk of harm to individual patients. However, the greatest danger is to public health in the broadest sense. Should patients decline to give their providers access to their medical records, misrepresent medical information or avoid treatment altogether, New York may lose both the individual and community-wide benefits health information technology promises. Both individual patient records and aggregated public health data will be increasingly susceptible to error due to incomplete or inaccurate information. Doctors may unwittingly base diagnoses on false or misleading information, leading to treatment decisions that are not in the patient's best interest—or that cause actual harm. Data compiled for the purpose of analyzing public health issues will be skewed, underreporting information from the records of those patients with greater privacy concerns. In turn, this phenomenon would lead to the flawed assessment of public health problems and trends.

Americans want their medical information—whether in paper or electronic form—to be held in private with their medical providers.[22] Most patients expect that medical privacy is far more vigorously protected by law than it actually is.[23] All health care consumers have an interest in the confidentiality of their medical records; but for some, privacy safeguards are essential when they seek treatment and services for sensitive health care issues related to HIV/AIDS diagnosis and treatment, reproductive health, substance abuse, mental health, genetic conditions, sexual assault, and domestic violence.[24] Minors seeking care have perhaps the greatest need of assurance that their medical information will be held in confidence.[25] Studies indicate that minors will avoid or delay seeking care if they believe that their parents will find out.[26] As records become electronically linked—office to office, region to region and ultimately state to state—the need to ensure that adequate privacy protections are in place grows in proportion to the sheer number of people, including legions of non-medical personnel, who have push-button access to a patient's entire medical history.

New concerns will arise as electronic networks allow patients direct access to their own medical records, via provider-created portals or through contracts with free-standing Personal Health Record (PHR) systems such as Microsoft Health Vault.[27] Patients may also have access through smart phone applications and other means not yet envisioned.[28] These powerful tools will permit patients to identify and correct errors in their records, collate and track their own health information retained in multiple sources, and ultimately enter their own health-behavior information in electronic databases.[29] Some regional health information organizations have already considered providing patients access to their own health information via the use of commercially-available PHRs.

The proliferation of personal health records raises questions about privacy that have been largely unexamined and wholly unresolved. Which sorts of records are governed by New York State privacy laws, which by HIPAA, and which by the Federal Trade Commission? Can patients rely on the same protections of medical information held by PHRs as they do for information held within a doctor's file cabinet or computer? What protections do patients have against disclosure or data mining[30] by a third-party vendor of a smart phone app when the vendor may not be required to comply with federal privacy standards?[31] Would such information be protected if requested pursuant to subpoena? What if records are accessed or downloaded by a patient on his or her employer's computer? New York State must thoughtfully and deliberately consider the issues raised before entering this uncharted territory.

PART 2: Developing New York's Electronic Health Information Exchange

Efforts to create a network of shared electronic health records began in earnest in April 2004 with an executive order from the Bush administration setting adoption of interoperable electronic health records by 2014 as a national goal.[32] The executive order also established the Office of the National Coordinator for Health Information Technology in the Department of Health and Human Services, and a strategic plan and funding streams for state and national HIE programs.

During the Bush years, national policy for developing an electronic medical records system focused largely on market-based, free-enterprise strategies and on initiatives undertaken by individual states. The Obama administration brought significant resources to this undertaking—including funding, policy guidance and national organization—through the Health Information Technology for Economic and Clinical Health Act (HITECH), passed in February 2009.[33] While HITECH greatly increased funding for health information technology, it also transformed the federal government's approach to privacy and consent, establishing new protections for personal health privacy and substantially extending the limited protections of HIPPA.[34]

New York State's health information technology initiatives also date to 2004, with passage of the Health Care Efficiency and Affordability Law for New Yorkers Capital Grant Program (HEAL NY).[35] HEAL NY's primary objective was "implementing a 21st Century health information infrastructure."[36] New York State established the Office of Health Information Technology Transformation in 2007 to begin "building an infrastructure to share clinical information between patients, providers, payers and public health entities." This infrastructure will ultimately be integrated into a statewide network and into the planned national network.[37] New York State has since invested more than $840 million to develop HIT networks throughout the state.[38] A state-funded grant program now funds 12 Regional Health Information Networks (RHIOs) that facilitate patient record-sharing.[39] At present, more than 65,000 health care providers participate in RHIOs.[40]

As New York State began to develop the health information exchange, the state introduced a process for developing policies and procedures that govern patient consent and privacy.[41] Stakeholder meetings took place even as some RHIOs recruited providers and patients. The accelerated policy development process left little time for careful consideration of policy debates about privacy and consent happening at the federal level and across the country, or of rapidly evolving technological capabilities.

The state's operational plan acknowledges that "New York State currently has a fragmented legal and regulatory framework for the exchange of Health Information."[42] Nevertheless, New York has not carried out a comprehensive analysis of state law as it relates to the state's own HIE policies and procedures governing patients' privacy interests.[43] Likewise, the state has not provided any legal analysis or guidance to RHIOs, HIEs or providers to ensure that they implement HIE in ways that comply with existing law.[44]

New York faces a daunting challenge: creating an electronic information exchange while making prudent choices in design and policy that ensure compliance with state and federal laws, and incorporating evolving technological capacity to segregate and protect patient data. This balancing act

is no small feat. However, two early, critical policy choices made by the statewide collaborative process have created significant problems affecting electronic record sharing in the state: (1) an inadequate patient consent protocol that gives patients little choice in whether and how to participate in health information exchange; and (2) an all-or-nothing approach to data sharing that prevents participating patients from controlling the dissemination of their medical information.

Patient Consent to Inclusion and Use of Medical Records in an Electronic Information Exchange

Administrators of an HIE could employ any one of a variety of patient-consent models to allow for greater or lesser deference to patients' wishes regarding the inclusion of their medical information in a network and the ability of providers or other entities to gain access to that information.[45] Most models give some measure of control to patients—an option to "opt-in" or to "opt-out." With opt-in models, patients must do just that—provide explicit consent that their records can be linked to a network or electronically accessed. In an opt-out model, all patient records are automatically shared unless the patient opts out by electing to withdraw from the program. New York State describes its patient consent protocol as an opt-in model,[46] but it is actually a hybrid that incorporates elements of the two models just described.

There are two stages in New York's protocol for establishing access to electronic medical records: First, patients are linked to a patient registry (or patient locator system) and their records become accessible through an HIE. Second, a provider or other entity seeks access to those records. When a health care provider joins an HIE, information that identifies each of the provider's patients is automatically linked to a search system that permits those who have access to the network to identify patients in the network. Identifying information could be demographic (an address) or some kind of unique patient identifier. At this point, patient information is accessible through the HIE. Patient consent is not sought at this stage.[47]

New York, in effect, requires the automatic enrollment of all patients of providers participating in an HIE. Patients may not opt out (and therefore their identifying information is available to those with access to the network); and they are not notified that their information is now available through the HIE.

New York employs an element of the opt-in model once a provider or other entity seeks access to a patient's information through the HIE. In the course of ordinary treatment, a patient's affirmative consent is required before a provider can access that patient's records through the HIE.[48] Generally, patients are presented with a consent form for release of their medical information with the paperwork filled out upon arriving in a provider's office, along with a pamphlet that explains the benefits of the electronic record-sharing program and provides a short statement about potential risks.[49]

New York State has adopted a model consent form, but HIEs across the state may use a variation of this form provided it conforms to basic minimum standards.[50] The consent form asks the patient to opt-in—to permit the provider to access all of the patient's records available throughout the network. In addition, New York's model patient-consent form cautions patients that by placing their signature on the form, they surrender any and all rights under New York and federal law regarding the dissemination of, and access to, sensitive information in their medical records that is accessible through an HIE.[51]

Patient consent, in this context, serves as blanket permission to release all medical information, notwithstanding the type of treatment received; the date it was provided; the facility at which treatment was received; or even the relevance to the medical condition for which treatment is sought. (See discussion of patient control and granularity below.) What's more, depending on

the consent form used by the HIE, the patient may be consenting to access by affiliated providers as well—ranging from the doctor's practice, a hospital, affiliated health facilities or to all providers in the network.[52]

On the surface, the distinction between mandatory inclusion of patient information in an HIE and the option to allow a provider access to that information may seem slight. However, there are two key issues to consider: First, some patients may seek to avoid being included in a patient locator system by going to a provider who is not enrolled in the network or by paying for services out of pocket.[53] Some may refuse care altogether to avoid being part of a state or national "listing."[54] Second, and, perhaps more important, some patients may face actual harm from inclusion in a patient registry that reveals demographic information such as a residential address.

The linking of one's medical records to an electronic network may provoke fear of unauthorized access or breach that could allow a hacker to gain access to patient identities or entire medical histories—either as a wholesale medical records theft or in pursuit of information about a specific patient. And this fear may be well founded. The mere inclusion of demographic information in a directory of existing records, regardless of whether complete medical records are made accessible, can pose an unacceptable risk to patients. Take, for example, those patients at risk of domestic violence, harassment, stalking or with other special concerns about confidentiality, such as public figures or crime victims.[55] The ability to glean an address or indeed any information that may reveal a patient's location may cause irreparable harm.

New York maintains that this two-stage process satisfies the myriad laws that require patient consent before information can be shared with a third party.[56] This is highly debatable. Informed consent requires prior notice that is clearly communicated: presenting the consent form amidst a sheaf of insurance documents, HIPAA releases and other paperwork fails to meet this basic criterion. What's more, the automatic disclosure of patient identifying information to an HIE most likely constitutes a violation of New York State law, which requires patient consent whenever patient information (including patient identifying information) is disclosed to a third party.[57]

In many respects New York's patient consent protocol represents a radical departure from current law and practice. The protocol effectively eviscerates decades of carefully considered and crafted law, replacing special consent requirements and confidentiality protections for information related to sensitive conditions such as HIV, substance abuse and others with one all-or-nothing consent form.[58]

New York's share-first, ask-later approach is based on a questionable interpretation of the law.[59] Under this reading of the law, HIEs and RHIOs would be exempt from rules regarding third-party disclosure because they are considered "practitioners or other personnel employed by or under contract with the facility[.]"[60] To date, no case law recognizes organizations like HIEs and RHIOs as exempt from the prohibitions against third party disclosure. There is, however, a considerable body of law that upholds the restriction on dissemination of patients' records to third parties.[61]

A new patient-consent protocol

Once provided with information and guidance regarding health information exchange, patients must be afforded clear options regarding the inclusion of their identifying information and medical records in an electronic health information network, and for sharing that information.

In light of the concerns outlined here, it is the position of the NYCLU that the state should revisit its policy on uploading individual medical information to a shared network and adopt a requirement that such information cannot be uploaded without affirmative patient consent. Should the state reject this reform, it should at least allow patients to affirmatively opt out of the system at any time so that their

medical information is not included in the network. Patients should also be afforded the opportunity to mask or exclude demographic information from a patient registry or locator system while retaining the ability to share medical records with specific providers.[62] Indeed, one can easily choose to have an unlisted telephone number; why not have "unlisted" medical records as well?

Once a patient's medical information is included in the network, the state should offer three clear options regarding provider access to such information:[63]

> **Opt in:** Patients consent to make information in their medical records available to specific, designated providers through electronic information networks.
>
> **Opt out:** Patients prohibit under all circumstances access to their medical information through electronic information networks.
>
> **Opt out with exception:** Patients consent to make information in their medical records available through electronic information networks only in the case of a medical emergency.

In addition to offering these patient consent options, patients must be notified in advance of a provider's joining an electronic records exchange. This notice must clearly explain the manner in which electronic medical records will be accessible, as well as the steps a patient can take to exclude or limit the release of their medical information through an HIE. This same notice requirement should apply when the network of providers with access expands, as for example, when a hospital that has previously obtained consent from a patient adds new affiliates. Under current consent policies, these affiliated providers may gain access to the patient's records. It should not be left to the patient to continually check a website to find out whether new providers have joined an exchange network.

BREAKING THE GLASS: PATIENT PRIVACY IN A MEDICAL EMERGENCY

In a medical emergency where a patient is unable to authorize access to his or her medical records, New York's policy purports to create a limited exception to the law that patient consent is required before the release of such records. Under the state's "break the glass" policy, a provider who asserts a need to see a patient's medical record in such an emergency can access the patient's entire medical records without consent.[64] In addition to the lack of clear authority to promulgate such an exception, the "break the glass" exception poses myriad problems. Even sensitive medical information subject to specific state and federal confidentiality protections may be accessed, regardless of whether the provider needs to see such information in order to treat the patient.

In all circumstances, New York law requires patient consent before medical information can be released to a third party; there is no "emergency" exception to the law's straightforward requirement.[65] Patients and providers may see the value in giving an emergency care doctor access to medical information that could improve patient care. However, only the legislature has the authority to create an exception under the law for emergency care. Should the legislature choose to do so, such an exception should be limited to allowing providers access to only that information that is relevant to the emergency.

Individuals may not fully appreciate the potential harm in having their health information accessible until they no longer have the ability to reduce that risk. Consider the patient who chooses a provider for treatment of a sensitive, personal nature because the provider does not participate in an HIE, only to learn at a later date that the provider subsequently made his patient files available through a medical records network. The same concern may arise when records in a regional health information exchange are included in a statewide network. Patients who are willing to include their medical information in a local HIE may want to prevent, or to limit, the dissemination of that information through a regional, state or national health information network.

Patient Control of Information-Sharing

New York State has made two critical policy decisions in creating the state's electronic health information exchange infrastructure. The first was to allow patient information to be uploaded to the network without patient consent. The second was to adopt an "all-or-nothing" model of sharing information.[67] When a patient consents to allow a provider to access her medical information through an HIE, that provider will receive any and all information contained in her record, regardless of who provided the treatment; the type of care received; the date it was provided; or even its relevance to current medical treatment. Consent automatically confers access to all information in the patient's record, including substance abuse treatment, mental health conditions, abortion and other reproductive health care, and testing and treatment for sexually transmitted infections. In addition, consent is generally granted to entire facilities; patients cannot specify which doctors may—or may not—access their records.

This kind of blanket consent stands in stark contrast to the nuanced controls possible in the world of paper records. And despite New York

The state's justification for this policy appears to be based on another section of the public health law, which in fact only permits an exception for providing emergency treatment in the absence of informed consent,[66] not access to records. Even if the law could be interpreted to give a provider access to medical information by virtue of his authority to treat without informed consent, the provider would only be entitled to information material to emergency treatment. But the infrastructure of New York's network (an "all-or-nothing" approach to information sharing, as described herein) does not provide a means to separate out and allow access to only that information that is directly relevant to emergency treatment.

New York's model consent form allows patients to decline consent for medical providers to access their electronic medical records in a medical emergency. But exercising this option is predicated on knowing that the network—and the break the glass policy—exists. Patients are likely unaware that their demographic information is electronically accessible or that their medical information can be accessed in an emergency without their consent. Consider the patient whose doctor links his practice to the electronic network the day after the patient's annual visit. The patient will not learn that his records are part of an electronic system until his next annual check-up, a year later. The only routine opportunity a patient has to decline provider access to her medical records in a break the glass scenario will be during some later medical visit long after the records have become accessible through the system.

State and federal law requirements that providers share only that information which is medically necessary for the patient's current treatment, New York's current policies and procedures do not allow the sharing of information to be limited in this way. It is possible, however, to realize the public health benefits of an electronic health information network without requiring patients to completely surrender control over information contained in their medical histories. These two interests are not irreconcilable; they must be balanced.

This principle of balance informs an emerging national model regarding the collection and dissemination of medical records in electronic information networks.[68] This model recognizes that patients must have discretion regarding which information is shared with what health care providers. And patient choice, in this context, requires the capacity to segregate data. Policy technicians use the phrase "granular control" to describe this concept.[69]

After exhaustive deliberations—including no fewer than nine public hearings conducted over the course

GRANULAR CONTROL OF PATIENT INFORMATION

The ability of an electronic data-sharing system to sort and segregate information is often referred to as granular control or data segmentation. Patients and providers have the ability to exercise granular control over health data when they can specify which pieces of data from a patient's medical record to include or block when that record is conveyed to a third party. In systems capable of granularization, personal health information ideally can be sorted by data type (e.g., a blood test, a diagnosis, a procedure); by provider (e.g., a gynecologist, a psychologist, an internist; or medical providers vs. office staff); by time range (e.g., between x date and y date, within five years, or for a 24-hour period for emergency treatment); and by purpose (e.g., payment, care delivery, quality improvement, clinical research or health services research).

Federal and state law provisions mandating confidentiality for certain types of medical information make granularity an essential component of electronic health information exchange. Beyond the confidentiality rules that apply to narrow categories of medical information like HIV and substance abuse treatment, patients may have a desire to exercise granular control over information that they deem sensitive for a variety of reasons, including fear of discrimination or misuse, a personal preference for privacy, a valuation of fundamental autonomy, or because the information is erroneous. Likewise, providers may appreciate granularity so that they can limit the vast amount of information they may be expected to review for any given patient. On the other hand, providers may have concerns about the level of confidence they can have in relying on an "incomplete" medical record where certain information may be restricted from their view at the request of a patient.

Allowing for granular control in health information exchange presents technological, conceptual, and implementation challenges that policymakers must carefully grapple with to achieve a balance that satisfies legal requirements, the need for patient acceptance and engagement, and provider confidence.[70]

PATIENT CONTROL OVER SENSITIVE HEALTH INFORMATION

Once a patient consents to allow a provider to gain access to his or her medical records, the provider gains access to everything in that patient's records—there is no way to ensure that the provider only sees information that is relevant to current treatment. This "all-or-nothing" approach to data sharing forces patients to choose between giving a current provider access to their medical records and maintaining future control over sensitive health information. Once sensitive information enters into the patient's general medical record, there is no way to exclude it again. When patients are unable to exercise granular control over information in their health records, there are serious ramifications.

Sexual Assault Care

Consider, for example, a patient who was raped in her twenties, and briefly took antidepressants to cope with trauma. New York's all-or-nothing system does not allow her to restrict access to this sensitive information to those providers for whom it is medically relevant. If she were to seek treatment for a skin condition, she cannot share current medical information with her dermatologist without also revealing this traumatic incident in her past. Each time the need for medical care arises, she must determine whether or not to provide access to her medical records because her assent means informing the provider that she had been the victim of rape.

Reproductive Health Care

Abortion is controversial for some, yet 3 in 10 adult women will have an abortion at some point in their lives.[73] A woman who terminates a pregnancy may be concerned about making that information available to anyone with access to an electronic network that contains her medical information. She may want her current medical providers to have access to any information in her medical history that may be relevant to her treatment, but she cannot do so without losing the power to shield information about her abortion from future providers 10 years hence.

Substance Abuse Treatment

The level of stigma that attaches to those who have struggled with substance abuse is profound. For this reason, information about substance abuse treatment is accorded the most stringent confidentiality protection by law. While information about that treatment may be relevant for a period of time, it becomes irrelevant for the medical provider treating that patient for a wholly unrelated condition 10 sober years later. The indiscriminate release of that medical history could undermine both personal and professional relationships, and the potential harm is not limited to social stigma. Including information about past treatment opens the door to misuse of medical information. A provider may refrain from prescribing medically appropriate pain relief to a patient who has been treated for substance abuse many years in the past based upon an assumption that the patient is exhibiting "drug-seeking" behavior.

of six years—the National Committee on Vital Statistics (NCVHS) concluded that patients' confidence and trust in the integrity of an electronic health information network is essential to its effectiveness; and that creating trust in this enterprise requires giving patients control over the release of personal medical information. In 2010 the chairperson of the NCVHS sent a letter to Kathleen Sebelius, secretary of the U.S. Department of Health and Human Services, making a strong case that the capacity to segregate (and therefore the ability to restrict) the release of patients' health care information must be context specific, and that "granular segregation" of that information must be responsive to the specific concerns of patients.[71] The Office of the National Coordinator of Health Information Technology, a unit in the U.S. Department of Health and Human Services, has taken a position that is consistent with the analysis set out in the NCVHS letter.[72]

New York policymakers insist that existing technological infrastructure does not have the

THE MINEFIELD OF ADOLESCENT CONSENT

For adolescents and their care providers, the failure to allow for patient control of sensitive medical information poses an insurmountable obstacle to the delivery of essential medical care. In New York State, minors can consent to specific types of health care, including reproductive health and certain mental health treatment, without parental involvement (sometimes referred to as "minor-consented services").[75] While parents have a right to access their children's medical records generally, parents and future providers may not obtain information about such minor-consented services, and doctors may not share such information, without the minor's permission. Ideally, a system should allow access only by health care providers who have received the minor's consent, while shielding that information from parents who routinely access their child's other medical records. New York does not allow segregation of data in this way. As a consequence, many RHIOs simply exclude the medical records of all minors between the ages of 10 and 18 from the network altogether—a practice that protects minors' privacy rights but deprives them of the potential benefits of health information exchange.[76]

In the case of a 15-year-old seeking testing and treatment for herpes, for example, his pediatrician would like to enter this information in his chart. But the doctor has no way to prevent his patient's parents from gaining access to this information when they request copies of their son's medical records. In a world of paper records, the pediatrician could record this information on separate pages in the file but not release the confidential portion of her patient's records when she provides a copy of the records to a parent. In an electronic information-sharing system, the only way to protect this young person's confidentiality is to exclude the patient from the electronic-records system altogether. However, excluding only those minors who have exercised their right to consent on their own to certain types of medical care would signal—to providers, parents and others—that the minor has exercised that right, which then compromises the right. A system that allows for granular control of medical information would allow all minors to fully benefit from participation in HIEs, while ensuring that those who need it are assured confidentiality when they receive medical care of a sensitive nature.

capacity to allow patients to control access to medical information by data type, provider, time range or purpose. But the vendors of electronic health-information technology maintain that the capacity to segregate data in health records is well within reach.[74] The technological and logistical challenges of developing this data-segregation capacity are not insignificant—but neither are these challenges insurmountable.

National experts insist that the capacity to achieve granular segregation of patient health care information is a key goal—and a critical success factor—in the implementation of health information networks. Should the federal government mandate as a condition of funding that states develop the capacity to segregate patient health information—a likely possibility—New York State's electronic health information exchange system may find itself out of money and lagging well behind the emerging consensus regarding best practices.

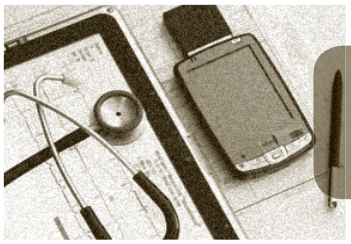
CONCLUSION

Electronic sharing of health records promises significant benefits. Ensuring that patients are able to control who has access to what parts of their medical histories is vital to this endeavor. Providers and public health advocates consider indispensible unfettered access to individual medical records that technology now makes possible.

However, well-established law and policy have recognized that patients have the right to control access to their private medical information. And indeed, patients have always controlled access to their medical records. Whether one doctor even knew that her patient was seeing another doctor depended entirely on what the patient chose to share.

Allowing patients to retain a measure of control over their medical records will increase confidence in the system's ability to safeguard confidentiality. This, in turn, will likely result in increased patient and provider willingness to participate in electronic health information exchange.

It is the position of the NYCLU that the state should revisit policy choices that affect the ability of patients to control the dissemination of their personal medical information. Accordingly, we offer 10 specific recommendations designed to accommodate patient concerns, and in turn, create a more reliable information-sharing system.



RECOMMENDATIONS

1. Ensure Patient and Provider Control of Access and Information-Sharing. The state must require that the electronic systems employed by HIEs have the capability to sort and segregate medical information in order to comply with guaranteed privacy protections of New York and federal law. The inability to exercise this kind of granular control over data poses an intractable barrier to realizing the full benefits of health information exchange. This limitation jeopardizes patient confidence, and it has led to the exclusion of young people's records from the network. Without the ability to exercise granular control over data in the network, people who receive medical care that requires strict confidentiality—for example, treatment of conditions to which stigma attaches—and the providers who deliver that care may choose not to share medical records in order to protect privacy. This increases the risk of harm to both patients and to the general public.

2. Offer Patients the Right to Opt-Out Altogether. The state should revisit its decision to upload patient information to the system without patient consent. Barring that, the state must adopt a policy that would allow patients to affirmatively opt-out of the system so that their medical information is not included in the network. The state should also ensure that a patient's identifying information is not accessible by those who have not obtained the specific consent of the patient. Providers who seek access to a patient's medical records do so by accessing a patient locator system that contains the names of patients and some other identifying information. Patient locator systems vary by HIE, with some HIEs utilizing patient addresses. For some, like domestic violence survivors, public figures, crime victims and celebrities, allowing that information to be accessible absent consent poses a significant risk of harm. For this reason patients must be offered the option of being "unlisted" in patient locator systems.

3. Require Patient Consent Forms to Offer Clear Information-Sharing Options. The state should revisit its policy on consent to allow greater patient control over how medical information is shared. Most consent forms used by New York State RHIOs are inadequate. They do not make clear that if the patient declines to sign the form, their information remains available in an emergency—frustrating both patients who want only emergency access and those who do not want even emergency access. Consent forms should offer patients three distinct options: to opt-in and allow providers access to their electronic medical records, to opt-out except in the event of a medical emergency, or to opt-out altogether.

4. Require Notice to Patients When Their Providers Become Data Suppliers. The state must adopt a policy mandating that providers notify patients when the provider links to HIE. In the absence of consent to upload patient information, patients must be notified when information about them from their provider initially become accessible through an HIE.

5. Guarantee the Right of Patients to Correct and Amend Information. Current state law allows patients the right to review and submit amendments to health information held by individual providers.[77] The practice of correction and amendment must be adapted to ensure that a correction to any error is automatically sent to any provider who has accessed the patient's medical records through an HIE. With paper records, a patient need only correct informa-

tion in one doctor's file. But the implementation of electronic records exchange amplifies the impact of any error, and erroneous information in a medical file can have a devastating impact on a patient's subsequent care.

6. Prohibit, and Sanction, the Misuse of Medical Information. The state should adopt a policy that prohibits and strongly sanctions the misuse of patient medical information obtained through an HIE. Providers misuse health information when they use that information to discriminate against, mistreat or withhold treatment from patients. New York's all-or-nothing system gives providers access to all of a patient's medical records—regardless of how old the information or how relevant it is for current treatment. State policies have rightly focused attention on the potential for breach as the state moves toward an integrated statewide network of medical records, but have not addressed the potential for the misuse of such information. New York must protect patients from potential bad actors—that small minority of providers who may abuse information out of fear, prejudice or malice.

7. Mandate Redisclosure Prohibitions for Third Parties. Current state policies do not require HIEs to warn those who access patient health information that redisclosing sensitive medical information without patient consent violates the law. While some RHIOs provide this notice as a matter of course,[78] state policy should require HIEs to explicitly communicate to third parties that redisclosure is prohibited and that there are penalties for violating this prohibition.

8. Prohibit Health Information Exchanges from Selling Data. The New York State Legislature should pass legislation prohibiting HIEs from selling patients' private health information. This prohibition should apply to records with or without a patient's personal identifiers. Medical information must not be used to target individuals or providers for promotional pitches or advertising campaigns; nor should HIEs be allowed to profit from the sales and marketing opportunities created by the release of information in patients' medical records.[79]

9. Carefully Regulate the Use of Commercially Available Personal Health Records (PHRs). A number of commercial vendors now offer patients the ability to collect, store and manage their own medical information online (such as Microsoft HealthVault[80]). Under existing law, it is unclear to what extent and under what circumstances these commercial entities are bound by HIPAA or New York State confidentiality laws.[81] State law should extend confidentiality obligations and protections to private entities that offer PHRs. If commercially available health records systems are offered to New Yorkers as a way for them to access and manage their own health information, the state must require that patients be warned of privacy risks. Patients must also be given access to their records without having to resort to a commercial vendor.

10. Step Up Public Outreach Efforts. The state should engage in a robust and effective public outreach campaign to fully inform New Yorkers about the implementation of HIEs. This public outreach and education program must not be a mere promotional campaign.[82] Patients require a basic understanding of what is at stake, both in terms of risks and benefits, before their medical information is linked to an HIE. This is particularly important because current New York State policy does not require consent before linking a patient's medical records to the network, and does not provide patients with an option to decline participation. Informed consent must be the cornerstone to health information exchange in New York, as has long been the case with sharing physical records. Consent cannot be considered informed if patients first learn about New York's network when they arrive at their doctor's office.

NYCLU'S INVOLVEMENT IN HIE IMPLEMENTATION IN NYS

The New York Civil Liberties Union attended one of a series of early stakeholder meetings convened by the New York State Department of Health (DOH) in 2007 to garner community input about the creation of an electronic health information exchange infrastructure. DOH has been the lead agency heading up this state effort, but the department delegated authority to develop the infrastructure and policies and procedures governing health information exchange to the New York eHealth Collaborative (NYeC). NYeC is a non-profit organization that was formed in 2006 to guide the development of the state's health information exchange and is described as a "public-private partnership."

NYeC and the DOH formed the New York Statewide Collaboration Process (SCP) to guide implementation and policymaking activities. The SCP is comprised of six work groups (Consumer and Provider Engagement, SHIN-NY Architecture, Privacy and Security, Public Health, Collaborative Care, and EHR Implementation) along with a Policy and Operations Council (POC), which reviews the activity of the work groups and reports directly to DOH and NYeC.

In 2008, the SCP issued a white paper outlining consumer consent policies and procedures, and the NYCLU responded to SCP's call for public comment. In response to the NYCLU's comments, and our organization's expertise regarding minors' right to confidential health care, the NYCLU was invited to participate in a subgroup formed by the Privacy and Security Work Group (PSWG), dealing solely with issues of minors' confidentiality and consent. The NYCLU participated in a smaller task force formed from that subgroup (the minor consent "Tiger Team"), charged with identifying solutions to the problem of protecting minors' confidentiality in HIE. The Tiger Team submitted a white paper in July 2010 calling for federal guidance on the issue to the Office of the National Coordinator for Health Information Technology (ONC). In February 2011, the NYCLU secured a position with the PSWG where it advocates on behalf of consumer privacy interests in the state's ongoing process of developing privacy and security policies and procedures.

ENDNOTES

[1] Mark A. Rothstein, *The Hippocratic Bargain and Health Information Technology*, 38 Journal of Law, Medicine & Ethics, 7, 7-8 (2010) ("In effect, physicians and patients entered into a 'Hippocratic bargain.' Physicians, explicitly or implicitly, said to their patients: "Allow me to examine you in ways that you would never permit any stranger, and tell me the most sensitive information about your body, mind, emotions, and lifestyle. These intrusions upon your privacy are essential in providing you with sound medical care.").

[2] The Statewide Collaboration Process, *Privacy and Security Policies and Procedures for RHIOs and their Participants in New York State Version 2.2* (April 1, 2011) ("NYS Privacy and Security Policies"), *available at* http://nyehealth.org/images/files/File_Repository16/pdf/final%20pps%20v2.2%204.1.11.pdf.

[3] *New York State Health Information Exchange Operational Plan*, New York eHealth Collaborative (NYEC) ("NY's Operational Plan") 6-10 (Oct. 26, 2010), *available at* http://www.nyehealth.org/images/files/File_Repository16/pdf/nys_hie_operational_plan_2010.pdf; *New York Regional Health Information Organizations (RHIOs)*, New York eHealth Collaborative (NYEC), last visited May 20, 2011, *available at* http://www.nyehealth.org/index.php/resources/rhios. New York State has chosen to accomplish this through a public-private partnership rather than through regulation or law.

[4] Security breaches have increased as the adoption of electronic medical records exchange has increased: the number of reported breaches has increased by 32 percent between 2010 and 2011. Each security breach costs a culpable institution an average of $2.2 million. Ponemon Institute, *Second Annual Benchmark Study on Patient Privacy and Data Security* (December 2011), *available a*t http://www2.idexpertscorp.com/assets/uploads/PDFs/2011_Ponemon_ID_Experts_Study.pdf. *See also* Nicole Perlroth, *Digital Data on Patients Raises Risk of Breaches*, N.Y. Times (Dec. 18, 2011) (reporting on the theft of a laptop computer from an employee of the Massachusetts eHealth Collaborative which potentially exposed over 13,500 patients' private data—an "identity theft gold mine."). Liability for security breaches often rests on health care providers who entrust not-for-profit groups like RHIOs because under federal law, "the legal burden of protecting patient data falls on . . . physicians and hospitals." *Id. See also* Kevin Sack, *Patient Data Posted Online in Major Breach of Privacy*, N.Y. Times (Sept. 8, 2011) (HHS revealed that the PHI of more than 11 million people has been "improperly exposed during the past two years alone. Since passage of the federal stimulus package, which includes provisions requiring prompt public reporting of breaches, the government has received notice of 306 cases from September 2009 to June 2011 that affected at least 500 people apiece. A recent report to Congress tallied 30,000 smaller breaches from September 2009 to December 2010, affecting more than 72,000 people. The major breaches — a disconcerting log of stolen laptops, hacked networks, unencrypted records, misdirected mailings, missing files and wayward e-mails — took place in 44 states."); Kevin Sack, *Patient Data Landed Online After a Series of Missteps*, N.Y. Times (Oct. 5, 2011) (The medical records of close to 20,000 patients were posted online for nearly a year because the hospital's billing contractor's marketing agent used an electronic spreadsheet with patient data as part of a skills test for a job applicant, who then posted the data on a public website. The marketing agent explained the breach as "a chain of mistakes which are far too easy to make when handling electronic data.").

[5] *See National Consumer Health Privacy Survey 2005*, California Healthcare Foundation, 17-21 (2005) (noting that one 1 of every 8 people surveyed engaged in some type of "privacy-protective behavior" such as going to a new doctor to avoid telling their regular doctor about a condition, paying their doctor not to record their health information, or deciding not to be tested out of concern that others might find out);

Deborah C. Peel, *Your Medical Records Aren't Secure*, The Wall Street Journal (Mar. 23, 2010), *available at* http://online.wsj.com/article/SB10001424052748703580904575132111888664060.html.

[6] *See* Jenna Wortham, *Facebook Glitch Brings New Privacy Worries*, N.Y. Times (May 5, 2010). After a spate of changes to privacy settings on Facebook, millions of users voiced their unease with the company's privacy policies. A leading privacy group filed suit against the company with the Federal Trade Commission; settlement of the dispute now requires Facebook to obtain "affirmative express consent" before allowing personal data to be shared more broadly than a user specifies. *See* Somini Sengupta, *F.T.C. Settles Privacy Issue at Facebook*, N.Y. Times (Nov. 29, 2011). *See also* Frances Martel, *Facebook Privacy Settings Attract Another Congressional Inquiry*, Mediaite.com (Feb. 5, 2011), *available at* http://www.mediaite.com/online/facebook-privacy-settings-attract-another-congressional-inquiry.

[7] Rothstein, *supra* note 1. The classic oath contained the wise dictum: "What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about." *See* Peter Tyson, *The Hippocratic Oath Today* (March 27, 2001), *available at* http://www.pbs.org/wgbh/nova/body/hippocratic-oath-today.html (translation from the Greek by Ludwig Edelstein, citing *The Hippocratic Oath: Text, Translation, and Interpretation*, by Ludwig Edelstein. Baltimore: Johns Hopkins Press (1943)). A modern version of this portion of the oath holds: "I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know." *Id.* (The modern oath was written 1964 by Louis Lasagna, Academic Dean of the School of Medicine at Tufts University and has been used in many medical schools).

[8] Audiey C. Kao & Kayhan P. Parsi, *Content Analyses of Oaths Administered at U.S. Medical Schools in 2000*, 79.9 Academic Medicine, 882-87 (2004), *available at* http://journals.lww.com/academicmedicine/Fulltext/2004/09000/Content_Analyses_of_Oaths_Administered_at_U_S_.15.aspx?WT.mc_id=EMxALLx20100222xxFRIEND# (stating 129 of a total 141 medical schools in the United States "explicitly addressed the need for physicians to protect a patient's confidentiality" in the oath administered to students); In addition, the AMA describes its own Code of Medical Ethics directive on confidentiality in this way: "Information disclosed to a physician during the course of the patient-physician relationship is confidential to the utmost degree." *See Patient Physician Relationship Topics: Patient Confidentiality*, American Medical Association, last visited May 18, 2011, *available at* http://www.ama-assn.org/ama/pub/physician-resources/legal-topics/patient-physician-relationship-topics/patient-confidentiality.page.

[9] Health Insurance Portability and Accountability Act, Public Law (PL) 104-191, 110, § 1936 (1996); *See* Angela Choy, Leigh Emmart, Joanne Hustead, & Joy Pritts, *The State of Health Privacy: A Survey of State Health Privacy Statutes*, Health Privacy Project, Georgetown University (2002), *available at* http://ihcrp.georgetown.edu/privacy/pdfs/statereport1.pdf (part 1) & http://ihcrp.georgetown.edu/privacy/pdfs/statereport2.pdf (part 2).

[10] American Recovery and Reinvestment Act (ARRA), Public Law No. 111-5, §§ 13401-13424 (2009) (codified at 42 U.S.C. § 17935).

[11] *See e.g.,* confidentiality requirements applicable to information about patients receiving federally-funded family planning services at 42 C.F.R. § 59.11 ("All information as to personal facts and circumstances obtained by the project staff about individuals receiving services must be held confidential and must not be disclosed without the individual's documented consent, except as may be necessary to provide services to the patient or as required by law, with appropriate safeguards for confidentiality."); confidentiality requirements applicable to information about those receiving substance abuse treatment at 42 U.S.C.A. § 290dd-2 ("Records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any program or activity relating to substance abuse education, prevention, training, treatment, rehabilitation, or research, which is conducted, regulated, or directly or indirectly assisted by any department or agency of the United States shall … be confidential and be disclosed only for the purposes and under

the circumstances expressly authorized under subsection (b) of this section . . ."); confidentiality requirements applicable to genetic testing contained in the Genetic Information Nondiscrimination Act of 2008 (GINA), Public Law No.110–233, 122 Stat. 881 (codified in scattered sections of 26 U.S.C.A., 29 U.S.C.A., and 42 U.S.C.A). *See also* Salvatore J. Russo & Wayne A. McNulty, *Analysis of the Disclosure of Health Information to and Through Health Information Exchanges in New York State*, New York City Health and Hospitals Corporation Office of Legal Affairs (2011) ("HHC Analysis") (outlining provisions in federal and New York State law that add additional protections).

[12] *See e.g.,* Choy, Emmart, Hustead & Pritts, *supra* note 9.

[13] "[H]aving pioneered the use of statutes to protect the confidentiality of medical records, New York has been zealous in safeguarding those privacy concerns." *Wheeler v. Commissioner of Social Services of the City of New York*, 223 A.D.2d 4, 8-9 (N.Y. App. Div. 1997) (citing various New York State statutes protecting confidentiality: Mental Hygiene Law §§ 33.13, 33.16; New York Public Health Law §§ 18(6), 2805-g(3); 8 N.Y.C.R.R. § 29.1(b)(8); and 10 N.Y.C.R.R. § 405.10.).

[14] *See* New York Public Health Law § 18(6).

[15] *Id.* ("Whenever a health care provider, as otherwise authorized by law, discloses patient information to a person or entity other than the subject of such information or to other qualified persons . . . [a]ny disclosure made . . . shall be limited to that information necessary in light of the reason for disclosure. Information so disclosed should be kept confidential by the party receiving such information and the limitations on such disclosure in this section shall apply to such party."); HHC Analysis, *supra* note 11, at 4-5 (quoting *Genetic Testing and Screening in the Age of Genomic Medicine*, New York State Task Force on Life and the Law, 259 (2001) (discussing New York Public Health Law § 18, which prevents health care providers from giving information to third parties unless the patient gives written consent, and provides that "disclosure must be limited to that information necessary in light of the reason for the disclosure.")).

[16] New York Civil Rights Law § 79-l.

[17] *Id.* at § 79-j; New York Public Health Law § 18(1)(e); Mental Hygiene Law § 33.13.

[18] *Barriers to the Exchange of Pediatric Health Information*, NY eHealth Collaborative Privacy & Security Minor Consent Tiger Team, pages 7-8 (July 2, 2010) (describing numerous state law provisions and state and federal case law that create confidentiality rights for minors seeking health care on their own).

[19] *See* New York Public Health Law § 2306.

[20] *See* New York Public Health Law Chapter 45, Article 27-F.

[21] 45 C.F.R. § 160.103 (2006) (HIPAA provision that business associates of covered entities such as doctors or health insurers may be considered covered entities themselves, describing such business associates as " a person who . . . [o]n behalf of such covered entity or of an organized health care arrangement in which the covered entity participates . . . performs, or assists in the performance of . . . [a] function or activity involving the use or disclosure of individually identifiable health information . . . or . . . [p]rovides legal, actuarial, accounting, consulting, data aggregation[,] . . . management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates . . .").

[22] Melissa M. Goldstein & Alison L. Rein, *Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis*, Prepared for the Office of the National Coordinator for Health IT (March 23, 2010) at 24-25, *available at* http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_911197_0_0_18/ChoiceModelFinal032610.pdf (explaining the results of numerous

consumer polls and focus groups about expectations of privacy in the transition to electronic health information exchange).

[23] Indeed, a majority of Americans erroneously believe that in general their private information is subject to stricter protection than is the case. *See* Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities that Enable it*, page 4 (Sept. 2009), *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/Turow.pdf ("Americans mistakenly believe that current government laws restrict companies from selling wide-ranging data about them. When asked true-false questions about companies' rights to share and sell information about their activities online and off, respondents on average answer only 1.5 of 5 [questions about] online laws and 1.7 of the 4 [questions about] offline laws correctly because they falsely assume government regulations prohibit the sale of data.").

[24] *See, e.g., Privacy and Confidentiality in the Nationwide Health Information Network*, National Committee on Vitale and Health Statistics (June 22, 2006), *available at* http://www.ncvhs.hhs.gov/060622lt.htm.

[25] Jonathan D. Klein, M.D. et al., *Access to Medical Care for Adolescents: Results from the 1997 Commonwealth Fund Survey of the Health of Adolescent Girls*, 25 Journal of Adolescent Health, 120-125 (1999), *available at* http://download.journals.elsevierhealth.com/pdfs/journals/1054-139X/PIIS1054139X98001463.pdf (Although the title specifically refers to girls the study surveyed both young girls and boys).

[26] *See id.; see also* Diane M. Reddy et al., *Effect of Mandatory Parental Notification on Adolescent Girls' Use of Sexual Health Care Services*, 288 JAMA 710, 713 (2002) (describing a 2002 JAMA study that showed that nearly half of all sexually active teens visiting family planning clinics would stop using services if their parents were notified that they were seeking birth control. Another 11 percent reported that they would delay testing or treatment for STIs including HIV. Virtually all (99 percent) reported that they would continue having sex.)

[27] Numerous HIEs have contemplated relying on independent, free-standing commercial PHR products to satisfy the need to provide patient access to their own medical records. Some, such as Beth Israel in Boston, have implemented this. However, ironically, rather than being the easy answer, Google's recent announcement that it is ceasing operations of its Google Health illustrates the fragility of this sort of approach. Steve Lohr, *Google to End Health Records Service After it Fails to Attract Users*, N.Y. Times (June 24, 2011). In addition to the weak consumer uptake, this approach is rife with issues such as the absence of clear HIPAA protections, profit motives related to data mining on the part of a commercial enterprise, and inherent conflicts of interest. *See, e.g.,* Marianne Kolbasuk McGee, *5 Reasons Why Google Health Failed*, InformationWeek Health Care (June 29, 2011), *available at* http://www.informationweek.com/news/healthcare/EMR/231000697; Brian Dolan, *10 Reasons Why Google Health Failed*, MobiHealthNews (June 27, 2011), *available at* http://mobihealthnews.com/11480/10-reasons-why-google-health-failed.

[28] NY's Operational Plan, *supra* note 3, at 8.

[29] *Id.* at 8, 129.

[30] "Data mining" refers to process of "discovering interesting and useful patterns and relationships in large volumes of data." Christopher Clifton, *Definition of Data Mining*, in Encyclopedia Britannica, *available online at* http://www.britannica.com/EBchecked/topic/1056150/data-mining.

[31] Only covered entities are required to comply with federal privacy standards. Under the Health Insurance Portability and Accountability Act (HIPAA), a "covered entity" means "(1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction . . . " 45 C.F.R. § 160.103 (2006).

[32] Executive Order 13335, Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator, 69 Fed. Reg. 24059 (April 30, 2004).

[33] Health Information Technology for Economic and Clinical Health Act (HITECH), 42 U.S.C.A. § 17933 (2009).

[34] *Id.* (requiring the secretary of the Department Health and Human Services to designate an official in each regional office of the department to offer guidance and education on the rights and responsibilities that covered entities, business associates and individuals have related to federal privacy and security requirements for protected health information); *id.* § 17934 (stating that privacy provisions and penalties related to records apply to business associates of entities covered under HIPAA); *id.* § 17939 (mandating improved enforcement for violations under the HIPAA); *id.* § 1740 (stating that secretary of the Department of Health and Human Services shall provide a periodic audit of HIPAA covered entities and business associates); *id.* § 17935(a) (stating that a covered entity must respect the request of a patient to restrict distribution of health information if that patient has paid for medical services fully out of pocket).

[35] *Health Care Efficiency and Affordability Law for New Yorkers Capital Grant Program*, New York State: Department of Health (July 2010), *available at* http://www.health.state.ny.us/technology/efficiency_and_affordability_law.

[36] *Id.*

[37] *Request for Grant Applications, HEAL NY Phase 1: Health Information Technology (HIT) Grants*, New York State Department of Health and the Dormitory Authority of the State of New York (2005), *accessible at* http://www.health.ny.gov/funding/rfa/inactive/0508190240.

[38] The total investment to date in New York's health information infrastructure is more than $840 million, nearly $440 million in funding through the Health Care Efficiency and Affordability Law for New Yorkers Capital Grant Program, more than $280 million in private sector matching funds and nearly $120 million in other state and federal programs. *Health Information Technology (Health IT)*, New York State: Department of Health (March 2011), *available at* http://www.health.state.ny.us/technology.

[39] NY's Operational Plan, *supra* note 3, at 20.

[40] Statement made by David Whitlinger, Executive Director, New York eHealth Collaborative at a session entitled "SHIN-NY HIE Strategy" at the 2011 NYeC Digital Health Conference (Dec. 1, 2011).

[41] New York Statewide Collaboration Process (SCP) & New York Health Information Security and Privacy Collaboration (HISPC), Recommendations for Standardized Consumer Consent Policies and Procedures for RHIOs in New York to Advance Interoperable Health Information Exchange to Improve Care (Sept. 16, 2008) ("Consumer Consent White Paper"), *available at* http://nyehealth.org/images/files/File_Repository16/pdf/Consent_White_Paper_20081125.pdf ("Because New York is setting policy in the context of live implementations and is doing so through a statewide public-private collaborative model, there is a unique opportunity to stress-test new concepts that to date have largely been considered in either much smaller settings, on a theoretical basis, or in connection with proprietary or narrow technological approaches.")

[42] NY's Operational Plan, *supra* note 3, at 72.

[43] The New York eHealth Collaborative (NYeC) solicited public comments about the Operational Plan it submitted to the federal government. The NYCLU pointed to numerous statutory privacy protections the NYeC failed to consider. In its official response to the comments, NYeC simply noted that the comment had been received, but made no revisions to reflect it. Compare NYCLU Comments, New York eHealth Collaborative (NYEC), Comment for pages 78-79, page 4, *available at* http://www.nyehealth.org/images/files/File_Repository16/pdf/nyclu.pdf, and NYCLU Comments, NYeC Response to Comments, New York eHealth Collaborative (NYEC), page 15, *available at* http://www.nyehealth.org/images/files/File_Repository16/pdf/master_list_of_public_comments.pdf and NYeC, New York State Health Information Exchange Operational Plan (October 26, 2010), page 73, *available at* http://www.nyehealth.org/images/files/File_Repository16/pdf/nys_hie_operational_plan_2010.pdf.

[44] For example, the state asserts that "[a] single consent may be obtained to exchange all health information, including sensitive health information such as HIV, mental health, and genetic information," but provides no legal citation or analysis of existing law to support this broad—and erroneous—conclusion. *See* NY's Operational Plan, *supra* note 3, at 74. In fact, the legal protections for this type of information are not "waivable" through a single consent.

[45] *See* Goldstein & Rein, *supra* note 22 at ES-1 (setting forth five models of consent for inclusion of information in a network and for access to that information).

[46] *See id.* at A-5 (explaining that New York refers to its opt-in consent as an "affirmative consent model").

[47] *See* NYS Privacy and Security Policies, *supra* note 2 at 11 ("Affirmative Consent shall not be required for the conversion of paper patient medical records into electronic form or for the uploading of Protected Health Information from the records of a Data Supplier to a RHIO.")

[48] *Id.* at 9. One notable exception to the affirmative consent requirement is the state's "break the glass" policy, which allows a provider to gain access to a patient's medical records in the case of an emergency, as described herein. *Id.* at 10.

[49] *See Better Information Means Better Care: A Guide to eHealth for New Yorkers*, State of New York Department of Health, *available at* healthit.hhs.gov/portal/server.pt/.../CEE_Full_Tool_App_A508.pdf. Patients are generally given a stark choice between participating or opting out, with a warning that opting out means that they are also refusing access in emergency or "break-the-glass" circumstances. *See also* David Klein, *HIXNY Patient Consent and its Benefits*, Healthcare Information eXchange New York, last visited July 19, 2011, *available at* http://www.hixny.org/Providers/hixny-patient-consent-video (RHIO website video interview of Cindy Ciabotte, Director of Central Registration for Northeast Health Patient Care Division, describing how patients come in and sign up for the program: "We've had success integrating the consent process in the HIXNY patient choice within our current processes . . . for instance when we do the computer entry it is just one of the questions that we ask just like we ask other questions within the computer entry. When we have the HIXNY consent signed it's another consent that patients sign in the routine of signing paper work at the end of their registration, so we've integrated it."). A better model is one designed by the Rochester RHIO, which has attempted to provide notice to patients about its network prior to an office visit. *See e.g., How Do I Sign Up?*, Rochester RHIO, *available at* http://www.grrhio.org/patients/Signup.aspx (RHIO site page with links to a sample consent form describing to potential patients how they can sign up and advising them to complete the form next time they visit their doctor's office).

[50] *See* NYS Privacy and Security Policies, *supra* note 2 at 11; *see also* New York State RHIO Model Consent Form v.2.1 (effective April 1, 2011), New York eHealth Collaborative (NYEC) ("NYS Model Consent Form"), *available at* http://nyehealth.org/images/files/Policies/rhio_consent_form%20v%202.1.doc.

[51] *See* NYS RHIO Model Consent Form, *supra* note 50 (expressly warning that providers will be able to access information that "may relate to sensitive health conditions, including but not limited to: alcohol or drug use problems, birth control and abortion (family planning), genetic (inherited) diseases or tests, HIV/AIDS, mental health conditions, sexually transmitted diseases").

[52] The Long Island Patient Information eXchange (LIPIX) consent form, for example, provides patients with the choice of specifying specific providers who could be granted access or allowing all affiliated providers access to the patient's information. *See Consent For Release Of Health Information*, Long Island Patient Information eXchange (LIPIX), *available at* http://www.lipix.org/downloads/Consent.PDF.

[53] *See supra* note 34 (federal requirement that a covered entity must respect the request of a patient to restrict distribution of health information if that patient has paid for medical services fully out of pocket).

[54] The expansion of electronic records has already evoked notions of a kind of "big brother" centralized surveillance. *See* Ron Paul, *Statement Introducing the Protect Patients' and Physicians' Privacy Act*, House.gov, May 21, 2009, *available at* http://www.house.gov/apps/list/speech/tx14_paul/ppprivacy.shtml (introducing the "Protect Patients' and Physicians' Privacy Act," Congressman Ron Paul raising concerns that "unscrupulous politicians" or government employees may seek abusive access to patient records, and stating that the federal "medical privacy act" . . . actually protects the ability of government officials and state-favored special interests to view private medical records without patient consent.).

[55] National Committee on Vital Health Statistics (NCVHS) Letter to Kathleen Sebelius on Recommendations Regarding Sensitive Health Information (Nov. 10, 2010) at 13, *available at* http://ncvhs.hhs.gov/101110lt.pdf (noting that categories of patients at special risk in the event of access to demographic/locator information and/or identity information by those other than immediate providers of medical services include potential/actual victims of domestic violence or stalking, victims of violent crime whose attacker may seek to "finish the job," as well as celebrities and public figures).

[56] Consumer Consent White Paper, *supra* note 41.

[57] New York Public Health Law § 18(6).

[58] Most recently, for example, it took the New York State Legislature five years to change the state's HIV confidentiality statute. Public health officials, in the face of rising HIV infection rates in certain communities (and a set of federal recommendations issued by the CDC in 2006), launched an effort to amend New York's strong HIV confidentiality law (Public Health Law 27(f)) in order to simplify the forms used to obtain consent from patients to be tested for HIV. What ultimately amounted to minor tinkering with the language in the consent form was a process fraught with strident stakeholder debate over the course of four years and many different versions of the legislation. Various versions were considered each year. The first, Assembly Bill 11075, was introduced in 2006, but was not taken up by the Senate. In 2007, two bills were introduced, Senate Bill 6326/Assembly Bill 9195 and Senate Bill 7529/Assembly Bill 4813. The former passed in the Assembly but failed in the Senate. In 2008, again two bills were introduced, Senate Bill 8722/Assembly Bill 11461, and Assembly Bill 6825, which had no companion in the Senate. Neither version passed either chamber. In 2009, four different versions of the bill competed for votes and support among community stakeholders: Assembly Bill 4016, which had no companion in the Senate; Senate Bill 5660/Assembly Bill 7892 (which was revised once); Senate Bill 4484/Assembly Bill 7757 (also revised once); and Senate Bill 3293/Assembly Bill 11487. None of these bills passed in either chamber. Only two versions of the bill were introduced in 2010, Senate Bill 6734, which had no companion in the Assembly, and Senate Bill 8227/Assembly Bill 11487. The latter ultimately passed both chambers and was signed into law in 2010. With its current policies and procedures, it appears that DOH believes that it can bring about sweeping change without the kind of time-intensive deliberation and stakeholder input that was required for modifying the HIV test consent form.

[59] *See* Consumer Consent White Paper, *supra* note 41 at 17-21.

[60] New York Public Health Law § 18(6). *See also* HHC Analysis, *supra* note 11, at 5-6 (HHC argues that existing case law indicates that HIEs are not "personnel" but rather "independent contractors," and as such do not fall under the statutory exception to the general prohibition against disclosing patient information without written patient consent.).

[61] HHC Analysis, *supra* note 11 at 5-6.

[62] Indeed, health care providers have recognized that some patients may need extraordinary protection of their identity when they seek medical care. *See, e.g.,* SUNY Upstate Medical University Safety-at-Work Guide, page 14 (September 2011), *available at* http://www.upstate.edu/hr/document/saw_all_staff.pdf (guidelines for staff explaining the process for assigning patients with security concerns an alias); Mary-Katherine Lowes & Aviva Werek Sokolsky, *The Woman Abuse Safety Alert Tool: Harm Reduction Strategies in a*

Regional Health Centre, Mount Sinai Hospital, Toronto, Canada (November 2007), *available at* http://www.gce-oha.com/Client/OHA/healthachieve09_lp4w_lnd_webstation.nsf/resources/Patient+Safety/$file/Mt.Sinai+Submission+1.pdf (explaining the need to assign an alias to patients who are determined to be victims of domestic violence).

[63] New York's model consent form only gives patients two consent options, and expressly warns patients that unless they choose to deny consent altogether, "New York State law allows the people treating you in an emergency to get access to your medical records, including records that are available through" the HIE. *See* NYS Model Consent Form, *supra* note 50. Contrast this with the Bronx RHIO consent protocol. *Bronx Rhio Consent Form*, Bronx RHIO, *available at* http://www.bronxrhio.org/images/downloads/bronxrhio_consentform%20english.pdf (giving patients three clear options). Some RHIOs inform patients that they can decline to decide, effectively refusing to allow access for purposes of routine medical care while allowing access in emergency "break-the-glass" circumstances. *See Frequently Asked Questions*, Rochester RHIO, *available at* http://www.grrhio.org/about/faq.aspx ("Will Rochester RHIO help me in a medical emergency? Yes. In a medical emergency, you are likely to be seen by doctors who are not familiar with your medical history . . . If the emergency is life-threatening, these doctors would be able to access your medication history . . . PLEASE NOTE: If you have declined consent to a particular provider, that doctor – as well as all colleagues and staff members in the practice, hospital, or other organization where he/she is employed – will NOT be able to access your information even in a life-threatening emergency."); *see also RHIO Consent Form*, Southern Tier Health Link New York, *available at* http://www.sthlny.com/pdfs/STHLConsent_blank_Oct2010.pdf (advising that if a patient checks the box "I Choose Not to Consent or Cannot Decide at this Time," the named provider may have access to the patient's medical records in an emergency). The Brooklyn Health Information Exchange (BHIX) recognizes this third option even though it uses a version of the state's model consent form that only gives patients two options: to consent, or to deny consent. They acknowledge that a patient may opt not to choose at all, effectively denying access in all but emergency situations. The deficiency in this approach is that patients are not specifically informed on the form or in the accompanying materials that they actually have this third option. Interview with Irene Koch, director of BHIX, May 31, 2011. The NYCLU recognizes the benefit of the BHIX approach, which prompts staff to give patients a chance to revisit their decision at each visit, but believes that patients should not be left to figure out on their own that such an option exists.

[64] *See* NYS Privacy and Security Policies, *supra* note 2 at 10-11.

[65] N.Y. Public Health Law § 18(6).

[66] N.Y. Public Health Law § 2504(4).

[67] *See* Goldstein & Rein, *supra* note 22 at A-5 (In NY, "[c]onsent is considered to be all or nothing, meaning that any data contributed to the exchange could be made available (i.e., no ability to segment by data type).").

[68] *See, e.g.,* Gary Zegiestowsky, *Patient Privacy and Information Accessibility: A Necessary Balance*, NHIN Watch (June 28, 2011); J. Zoë Beckerman, Joy Pritts & Eric Golerud et al., *A Delicate Balance: Behavioral Health, Patient Privacy and the Need to Know*, California Health Care Foundation (March 2008), *available at* http://www.chcf.org/publications/2008/03/a-delicate-balance-behavioral-health-patient-privacy-and-the-need-to-know.

[69] *See* Howard Anderson, *Developing Standards for Access to Portions of EHRs* (April 8, 2011) (Interview with Joy Pritts on Granular Patient Consent), *available at* http://www.HealthcareInfoSecurity.com; *see also* Goldstein & Rein, *supra* note 22 at 7 (describing granularity by data type, provider, time range and purpose).

[70] *See* Goldstein and Rein, *supra* note 22 pages 7-12 for an extended discussion on granular control.

[71] NCVHS Letter, *supra* note 55.

[72] Letter on Privacy and Security Recommendations from Health IT Policy Committee to David Blumenthal, National Coordinator for Health Information Technology, 13-16 (Sept. 1, 2010) ("HIT Policy Committee Letter"), *available at* http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_6011_1815_17825_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/files/hitpc_transmittal_p_s_tt_9_1_10.pdf (Tiger Team Recommendation 4: Granular Consent); Melissa Goldstein & Alison Rein, *Data Segmentation in Electronic Health Information Exchange: Policy Considerations and Analysis*, Office of the National Coordinator for Health Information Technology (Sept. 29, 2010), *available at* healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy_and_security/1147.

[73] Guttmacher Institute, *Facts on Induced Abortion in the United States* (August 2011), *available at* http://www.guttmacher.org/pubs/fb_induced_abortion.html.

[74] In a letter to the National Coordinator for Health Information Technology, the HIT Policy Committee presented the findings of the Privacy & Security Tiger Team relating to the problem of granular control of data. The letter stated that technological capability for granular control is "emerging" and that it can "fulfill the aspiration of individual control." The HIT Policy Committee also noted that "many EHR systems have the capabilities to suppress psychotherapy notes" and "some venders offer the individual the ability to suppress specific codes." It notes that the technology looks "promising" and state that "[w]ith greater use and demand, this approach could possibly drive further innovations." HIT Policy Committee Letter *supra* note 72 at 13-16. On June 29, 2011 the Office of the National Coordinator for Health Information Technology held a committee meeting that focused on the technological capabilities of vendors for electronic health. A number of attendees made comments about the granularization capabilities of the technology offered by vendors. For example, Debabrata Mitra, an architect for Clinical Management for Behavioral Health Services (CMBHS) working for the Department of State Health Services in Austin, Texas explained that CMBHS has been facilitating the exchange of segmented data for nearly 10 years. *See Consumer Choice Technology Hearing (Transcript)*, U.S. Department of Health and Human Services Office of the National Coordinator for Health Information Technology Privacy and Security Tiger Team Health Information Technology Policy Committee, 44-53 (June 29, 2010), *available at* http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_945903_0_0_18/Consumer-Choice-Technology-Hearing-062910.pdf.

[75] *See* Consumer Consent White Paper, *supra* note 41 at 33 ("However, New York law permits minors to obtain certain types of health services (e.g., family planning, HIV testing, mental health or substance abuse treatment) based on their own consent, without the consent or knowledge of a parent or guardian ("minor consent services").") (citing numerous statutes and regulations).

[76] *See* NYS Privacy and Security Policies, *supra* note 2 at 13 (requiring minor consent at the time of service provision before information about that service can be exchanged). The practical effect of this provision is that RHIOs are not allowing for the exchange of information about those between 10 and 18 years of age. *See, e.g.,* FAQs, Health eConnections RHIO of Central New York, last visited May 19, 2011, *available at* www.healtheconnections.org/About/FAQs. ("What is the consent process for minors? Parents or guardians can provide consent on their children's behalf for ages birth – 9 years. New York State has special privacy protections for minors between the ages of 10 – 18, so a consent form is not provided and the health information for this age group is only accessible in a life-threatening emergency.").

[77] *See* N.Y. Public Health Law § 18(8) (right to challenge inaccurate medical information); N.Y. Mental Health Law § 33.16(g) (same right with regard to mental health, substance abuse, and developmental disabilities records). *See also* HIPPA, 45 C.F.R. § 164.526 (federal patient right to amend protected health information).

[78] The Brooklyn Health Information Exchange (BHIX) has taken a step in the right direction in this regard by including a brief statement on the log-in screen that warns users that redisclosure of the information

obtained through the RHIO may be prohibited by state law. BHIX Clinical Portal - User Log In Screen (screen shot on file with the NYCLU).

[79] The United States Supreme Court struck down a Vermont statute that prohibited the sale of doctor's prescribing information to pharmaceutical companies in *Sorrell v. IMS Health Inc.*, 131 S.Ct. 857 (2011) on the theory that restricting such sale violates the free speech protections of the First Amendment. We believe that the state could craft a prohibition on sale that would comport with *Sorrell*, particularly with regard to patient information, which was not at issue in *Sorrell*.

[80] *See* footnote 27 and accompanying text.

[81] *See, e.g.,* Robert Gellman, World Privacy Forum, *Personal Health Records: Why Many PHRs Threaten Privacy* (Feb. 20, 2008); National Committee on Vital Health Statistics (NCVHS) Letter to Kathleen Sebelius on Protection of the Privacy and Security of Individual Health Information in Personal Health Records (Sept. 28, 2009), *available at* http://www.ncvhs.hhs.gov/090928lt.pdf. *See also* Google Health's own homepage at http://www.google.com/intl/en_us/health/about/privacy.html, which states: "Unlike a doctor or health plan, Google Health is not regulated by the Health Insurance Portability and Accountability Act (HIPAA), a federal law that establishes data confidentiality standards for patient health information. This is because Google does not store data on behalf of health care providers. Instead, our primary relationship is with you, the user. . . Although Google Health is not covered by HIPAA, we are committed to protecting your privacy. Our Google Health Privacy Policy governs what information Google Health collects and how we use it, and any violation of that policy can be enforced by the Federal Trade Commission, which takes action against companies that engage in unfair and deceptive trade practices -- including violations of their privacy policies.").

[82] *See supra* note 49 and accompanying text (examples of educational materials specifying the benefits of the program, giving short descriptions of the program, and illustrating the ease of consenting to the program).

NYCLU
NEW YORK CIVIL LIBERTIES UNION

NEW YORK CIVIL LIBERTIES UNION

125 Broad Street, 19th Floor
New York, NY 10004
www.nyclu.org