



To: ILHIE Data Security and Privacy Committee
From: Colleen K. Connell, Executive Director, ACLU of Illinois
Date: 7/16/2012
Re: Patient Electronic Health Data Privacy and Security Policies – Written Testimony With Regard to Panels 1-7

I. Introduction and Summary of Testimony

My name is Colleen K. Connell and I am the Executive Director of the American Civil Liberties Union (ACLU) of Illinois. Thank you for considering my testimony as the Committee develops recommendations for the privacy, security, and consent management policies that may well govern the Illinois Health Information Exchange (ILHIE).

The ACLU is a non-partisan, non-profit organization dedicated to defending the liberties guaranteed by the U.S. Constitution and the Illinois Constitution as well as federal and state laws that protect individual rights. The ACLU has more than 20,000 members and supporters in Illinois and more than 500,000 members and supporters across the country.

The ACLU has substantial expertise on issues involving medical privacy and security of health records. For more than 40 years, through litigation and legislative activity, we have helped develop the contours of both the federal and state constitutional rights of individuals seeking or receiving health care, including their rights of autonomy and privacy. We have worked to protect individual rights in contexts that include reproductive health, the rights of survivors of sexual assault, the rights of survivors of domestic violence, the rights of minors, the rights of people with HIV/AIDS, and the rights of people with developmental disabilities and mental health diagnoses.

The Illinois General Assembly adopted the Illinois Health Information Exchange and Technology Act (ILHIETA) with the express legislative purpose of creating an electronic health information system to “improve the safety, quality and value of health care, to protect and keep health information secure, and to use the health information exchange system to advance and meet population health goals.”¹ The ILHIETA was enacted consistent with the federal HITECH ACT, which directs the development of a health information technology infrastructure that “improves health care quality, reduces medical errors, reduces health disparities, and advances the delivery of patient-centered health care.”²

Unquestionably, electronic health information technology (HIT) is transforming health care and promises to improve the effectiveness and the efficiency of the health care system. However, easily sharable electronic medical records threaten patient privacy and can lead to security breaches, misuse of information, and a loss of

¹ 20 ILCS 3860/5 (2010).

² Health Information Technology for Economic and Clinical Health Act, Division A, Title XIII of the American Recover and Reinvestment Act (ARRA)), Pub. L. No. 111-5, sec. 13101-13424, 123 Stat. 115, 228-279 (2009).

patient control over confidential and sensitive health information. This will undermine the patient well-being that was a primary impetus of the ILHIETA and the HITECH Act. Any loss of patient control over sensitive health information will reduce patient participation in the Illinois Health Information Exchange, thereby frustrating the additional legislative purpose of “full participation in the health information technology incentives available from the federal government.”

To achieve the full benefits promised by HIT, therefore, it is imperative that patient privacy be protected by all policies ultimately promulgated to govern the ILHIE. The ACLU offers the following recommendations in support of the goal of using HIT to improve the safety, quality and value of patient-centered health care in Illinois:

1. Protect the Right of Patients to Consent to the Sharing of Their Medical Records.

The Committee should recommend a policy that protects the right of all patients to decline to participate in the health information exchange altogether, or at the least, ensure that a patient’s identifying information is not accessible by those who have not obtained the **specific** consent of the patient. (Panel 1.)

2. Apply the Specific Patient Consent Rights Regarding Sensitive Health Information, as Codified in Numerous Illinois and Federal Laws, to the Operations of the ILHIE.

The Committee should recommend policies that continue the existing rights of patients to segment and then sequester from sharing specific elements of their patient records involving sensitive health information in such areas as intimate partner violence, substance abuse, HIV/AIDS, reproductive health, genetic testing and behavioral health. Patients and providers must maintain control over access to and sharing of all sensitive health records. Information sharing data systems must be designed to sort and segregate sensitive health information to comply with privacy protections under Illinois and federal laws. Without such protections, patients who need strict confidentiality with respect to certain treatments or tests – for example, for conditions or diagnoses to which stigma attaches – may choose not to share medical records, or may choose to forego that care altogether. Although information about certain categories of health care and testing are designated under Illinois law as having stricter limitations on dissemination, it is essential to adopt broader protocols that require granular consent for exchange of **any** information in patient medical records, as patients may need to segregate health information not covered by those laws. Moreover, this Committee should recommend continuing the protections in existing laws that advance patient control over their sensitive health information. (Panel 2 and Panel 3.)

3. Operational Protocols Should Assure That Patients Be Afforded Meaningful Choice as to Whether They Participate in the ILHIE.

The Committee should recommend a policy that requires that medical providers notify patients when the provider is preparing to link to the ILHIE; and further, that the provider seek the written consent of the patient before making his or her medical record accessible through the ILHIE. Consent forms should offer patients three distinct options: (1) to opt-in and to allow providers access to their electronic medical records, with the additional option of protecting the right of patients to segment sensitive health information and to restrict access to that sensitive health information; (2) to opt-out except in the event of a medical emergency, or (3) to opt-out altogether. The Committee also should recommend protocols that allow patients to restrict disclosure of PHI to payors, including restrictions consistent with the HITECH Act and federal and state genetic information non-discrimination acts. The Committee also should recommend protocol that allows patients to revoke their consent to sharing, thereby preventing future sharing. (Panel 5.)

4. Protect the Right of Patients to Confirm or Correct the Accuracy of Their Electronic Health Records.

Current law permits patients to review their medical records that individual providers hold. Consistent with existing law, the Committee should recommend a policy that allows patients to access their

individual medical records through the ILHIE and to suggest corrections or amendments. The Committee also should recommend a policy that requires medical providers and other entities with access to medical records, as a condition of participation in the ILHIE, to act promptly in response to a patient request that a record be corrected or amended; and if the record is corrected or amended, to ensure that any correction or amendment is automatically sent to any provider or entity who previously has accessed the patient's medical record through the ILHIE. (Panel 6.)

5. Patient Data Should Be Protected by Prohibiting the Sale of Data and Sanctioning the Misuse of Medical Information.

The Committee should recommend a policy, or if necessary, legislation, prohibiting providers or other entities who participate in the ILHIE or the ILHIE from selling patients' private health information; this prohibition should apply to records with or without a patient's personal identifiers. Medical information should not be used to target individuals or providers for promotional pitches or advertising campaigns; nor should providers or the ILHIE be allowed to profit from the sales and marketing opportunities created by the release of information in patients' medical records.

In addition, the Committee should recommend a policy that prohibits, and strongly sanctions, the misuse of patient medical information obtained through an HIE. Patients must be protected from that small minority who may abuse information out of fear, prejudice, malice, or desire for financial gain. (Panel 7.)

II. Protecting the Patients' Right to Consent to the Inclusion of Their Medical Records in the ILHIE and to Segment and Sequester Sensitive Health Information is Key to Achieving the Patient-Centered Goals of Health Technology Legislation and Essential to Protecting the Ethical and Legal Principles Undergirding Our Health Care System. (Panels 1 and 2.)

Protecting patient privacy is one of the most important considerations confronting the establishment of electronic health information exchanges. The Office of the National Coordinator for Health Information Technology issued a "Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information" that specifically provides that "individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use and disclosure of their individually identifiable health information."³ The HITECH Act grant to Illinois requires the State to incorporate the privacy and security provisions, at a minimum, of HIPAA, ARRA, and federal law concerning federally funded alcohol and drug abuse treatment programs, as well as work to coordinate privacy and security policies across state boundaries.

Although it will not be uncomplicated, respecting individual choice will assure that the ILHIE will:

- (1) comply with federal and state law that protects individual autonomy to make medical decisions and protect the privacy surrounding those decisions;
- (2) encourage greater participation and trust in the health care system through protection of a patient's most personal and private health information; and
- (3) ultimately produce public health gains by full participation in the health care system with more data available to benefit all.

A. Require Specific Patient Consent to Inclusion in the Health Information Exchange. (Panels 1 and 2.)

The ACLU recommends that the most effective way to protect patient privacy, consistent with existing statutory protections and the underlying common law and constitutional foundations, is to adopt a system that requires

³ Office of the National Coordinator for Health Information Technology "(ONC)", U.S. Department of Health and Human Services, *Nationwide Privacy and Security Framework For Electronic Exchange of Individually Identifiable Health Information*, 8 (Dec. 15, 2008).

each patient to specifically consent to the inclusion of his or her name in the Illinois Health Information Exchange (opt-in) and to further require the development of policies (and technology) that allow each patient to segment and sequester the health information included in his or her medical record, so as to allow the patient to determine what information should be included in a shareable health record and the opportunity to provide later, and specific consent before sensitive health information could be exchanged with a different health care provider through the ILHIE (opt-in with reservations).⁴ Furthermore, the patient should have the right to revoke any consent provided, thereby prohibiting future sharing of such information. Opt-in with the right to segment and sequester is consistent with constitutional and statutory protections, assures greater patient participation in the ILHIE, promotes more candid and comprehensive sharing of medical information with chosen providers, and ultimately best advances the statutory goals of improving a patient-centered health care system.⁵

Until the advent of electronic information technology, safeguarding patient privacy was relatively simple. Patient information was kept in physical form and, when asked to share patient information with another provider, a physician would secure the patient's permission, copy the relevant portion of the patient's file, and fax or deliver it to the other provider. Patient consent was required for each communication and patients retained control over which medical providers had access to what health information. Consensually providing sensitive health information to one physician did not – and it is the ACLU's position, still does not -- carry with it the patient's consent for the physician to share that information with all future providers any more than the patient's consent to one medical procedure constitutes consent to all future medical procedures.

Protecting patient privacy has been paramount to the delivery of care since at least the time of Hippocrates, who implored physicians to keep confidential any information obtained in the course of treating a patient.⁶ “In effect, physicians and patients enter into a ‘Hippocratic bargain,’” whereby patients tell physicians sensitive information about themselves, and then, consistent with that sharing of information, allow physicians to examine them in a way that no other stranger would be permitted.⁷

It is this concern for patient autonomy, coupled with the recognition of the harm people suffer from disclosure of sensitive personal information, which has led federal courts, including the U.S. Court of Appeals for the Seventh

⁴ For a complete discussion of the different consent options, including the advantages pertaining to an opt-in requirement, see Melissa M. Goldstein & Alison L. Rein, *Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis* (March 23, 2010) (hereinafter cited as “White Paper: Consumer Consent Options”), available at http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs. The ONC awarded The George Washington University Department of Health Policy a grant to conduct research and analyze key privacy, security, legal and policy questions presented by the adoption of electronic health records and the creation of health information exchanges. The GW Department of Health Policy produced two white papers, *Consumer Consent*, and Melissa M. Goldstein & Alison L. Rein, *Segmentation in Electronic Health Information Exchange: Policy Considerations and Analysis* (September 29, 2010) (hereinafter cited as “White Paper: Data Segmentation”). Both white papers provide extensive discussion of the consent options and the issues underlying the need for data segmentation.

⁵ White Paper: Data Segmentation at 64. Health information exchanges in Massachusetts, New York and Rhode Island all employ some variation of an opt-in. White Paper: Consumer Consent Options at 15-16. Massachusetts and Rhode Island also allow patients to identify which providers can and cannot contribute their personal health information to the exchange, a type of segmentation. White Paper: Consumer Consent Options at 16. In part because of increased patient trust and reflecting effective outreach efforts designed to secure patient consent, the Massachusetts eHealth Collaborative has an extremely high participation rate of more than 90% in the three communities it serves. White Paper: Consumer Consent Options at 51.

⁶ Mark A. Rothstein, *The Hippocratic Bargain and Health Information Technology*, 38 *Journal of Law, Medicine & Ethics* 7, 7-8 (2010).

⁷ *Id.* at 8. See also *Washington v. Glucksberg*, 521 U.S. 702, 720 (1997); *In re E.G.*, 549 N.E.2d 322, 326 (Ill. 1989).

Circuit to recognize “a constitutional right to the privacy of medical, sexual, financial, and perhaps other categories of other highly personal information.”⁸ Similarly, the Illinois Supreme Court has recognized that “[t]he confidentiality of personal medical information [is] . . . at the core” of our state constitutional right of privacy.⁹ This privacy guarantee is necessary because, to be effective as physicians, physicians are, and must be “privy to the most intimate details of their patients’ lives.”¹⁰

This authority prohibits government from collecting or accessing personal health information that identifies individuals who have accessed certain health care, for example, women who have had abortions.¹¹ Although the ILHIE does not contemplate creating a centralized electronic data base, allowing public health researchers access to individually-identifiable medical records that have protected status, would raise serious legal issues.

Advances in technology do not void these long-standing restrictions on sharing private medical information without specific patient consent because these restrictions reflect our most profound human values. This concern for harm, including loss of privacy, stigma, risk of physical harm, denial of health care, and loss of employment and other benefits underlies the many specific statutory restrictions on the sharing of medical data. The grave risk of harm posed by the disclosure and sharing of PHI is documented below in C, and in the testimony provided by the AIDS Legal Council, the AIDS Foundation of Chicago, and Planned Parenthood. These concerns underlie the ACLU’s position that the Committee should require not only patient consent to the sharing of medical records, but also require the creation of policies that require that patients control the granularity of their PHI by being allowed to segment and sequester particularly sensitive health information, and to limit the recipients of PHI and limit the duration of access.

B. HIPAA Does Not Mandate Sharing Protected Health Information through an Exchange Without Securing Additional Patient Consent.

The Illinois Health Information Exchange Legal Task Force Executive Committee identifies the HIPAA Privacy Rule as the baseline for the use and disclosure of protected health information (“PHI”). However, HIPAA should not be viewed as a “green light” to share all PHI through an exchange without additional patient consent.

It is important to recognize that HIPAA **permits** a covered entity to seek patient consent for uses and disclosure of PHI for purposes of patient treatment, payment, or health care operations, even though it does not require such consent.¹² Furthermore, the HIPAA Privacy Rule explicitly does not preempt state or federal laws, of which there are many, that require specific patient consent before certain protected and sensitive health information can be shared, including protected health information regarding substance abuse, behavioral treatment, and genetic testing.

Thus HIPAA recognizes that its protections are the minimum – not the maximum -- that must be provided. Incorporating specific patient consent plus the right to segment and sequester would incorporate specific limits on sharing that HIPAA already recognizes and would advance the improved patient-centered health care anticipated by the HITECH Act’s amendments to HIPAA as well as the legislative intent underlying the ILHIETA.

⁸ *Wolfe v. Schaefer*, 619 F.3d 782, 785 (7th Cir. 2010), citing *Whalen v. Roe*, 429 U.S. 589, 598-600 (1977).

⁹ *Kunkel v. Walton*, 179 Ill.2d 519, 537.

¹⁰ *Id.* at 537.

¹¹ See, e.g., *Planned Parenthood v. Danforth*, 428 U.S. 52, 70 (1976); see also *Gruenke v. Seip*, 225 F.3d 290, 301 (3d Cir. 2000) (minor student’s pregnancy status); *Doe v. City of New York*, 15 F.3d 264, 267 (2d Cir. 1994) (HIV status).

¹² See U.S. Dept. of Health and Human Services, Office for Civil Rights, *Summary of Privacy Rule*, 5 (2003). Available at <http://www.hhs.gov/ocr/privacy/hipaa/understandingsummaryprivacysummary.pdf> .

C. The Committee Should Recommend Policies that Continue the Existing Rights of Patients to Segment and Then Sequester Sensitive Health Information; and Further, to Decide Which Providers and Payors Will Have Access to That Information and For What Period of Time.

As I explained during my testimony on Panels 1 and 2, the ACLU recommends adopting a requirement that each patient specifically consent (or refuse consent) to the inclusion of their name in the Illinois Health Information Exchange (opt-in) and to further require the development of policies (and technology) that allows each patient to segment and sequester sensitive health information, such that an additional specific consent of the patient would be required before sensitive health information could be exchanged through the ILHE (opt-in with reservations). By ensuring the patient has the authority to sequester information he or she deems too sensitive to allow for blanket sharing to any new health care provider, the ILHIE will have addressed many of the patient privacy concerns that underlie federal and Illinois statutes and substantial case law. These laws individually and collectively provide more confidentiality for records describing certain types of health care, including but not limited to treatment for substance use disorders, behavioral health treatment, testing and treatment for HIV/AIDS, and reproductive health. And, as detailed in section D, below, special legal considerations require great segmentation and sequestering for minors' health records.

It is challenging to anticipate all of the many reasons people need to segment and sequester PHI. The ACLU's representation of clients in need of reproductive health care or HIV treatment, and clients who are survivors of intimate partner violence or sexual assault provide but a few examples of why patients must retain the right to segment and sequester **any** PHI the patient considers sensitive. For example, in the ACLU's litigation *Hope Clinic v. Adams*, No. 09-CH-38661 (Cir. Ct. Ill., Nov. 4, 2009), physicians and counselors attested to the harms suffered by teens when their parents learned of their pregnancies, including: severe beatings, being thrown out of the house, and having all financial support withdrawn. (Plaintiffs' Memorandum in Support of a Temporary Restraining Order at pp. 9-12. Similarly, victims of sexual violence may avoid seeking treatment after an attack because of stigma, embarrassment, fear of assailants and future attacks, and many other reasons.¹³ Allowing segmentation and limiting access to such records is particularly important in small and rural communities because providers may know the patient, the suspect, or both. Victims of intimate partner violence face similar risks and have a similar need to limit access to their records.¹⁴

Only the individual patient can accurately assess the risks created by broad access to PHI. If patients are not allowed to segment and sequester their records, many patients will not seek the medical care, and in some cases, the law enforcement protection they need.¹⁵

Both the Substance Abuse Legal Work Group and the Behavioral Health Legal Work Group recognize that HIPAA itself and parallel state laws impose substantial restrictions on the sharing of PHI without specific patient consent. Accordingly both Legal Work Groups recognize the need to incorporate specific patient consent requirements to enable the exchange of information through the ILHIE.

The ACLU supports the inclusion of specific patient consent requirements but does not share the conclusions of the Legal Work Groups that change should be promoted in existing state and federal law to eliminate or reduce the need for specific patient consent requirements. Instead, the ACLU supports broadening the specific patient consent requirements to require an opt-in before any PHI can be included and to further allow every patient who so wishes to segment and sequester any PHI that the patient considers sensitive, including but not limited to PHI that already is protected by state or federal law.

The ACLU recognizes that health care providers and other stakeholders in the ILHIE may generally support policies that allow access to patients' complete medical records through a system that minimizes technical, administrative and financial costs of participating in the exchange.¹⁶ These concerns for efficiency cannot

¹³ White Paper: Data Segmentation at 15.

¹⁴ *Id.* at 15.

¹⁵ *Id.*

¹⁶ *Id.* at 16.

override patient concerns for privacy and security. Our law recognizes higher values than speed and efficiency.¹⁷

Similarly, provider concerns about liability cannot override patient privacy needs. As discussed in the White Paper: Consumer Consent Options, provider concerns about liability are numerous and potentially contradictory.¹⁸ Although providers recognize the benefit of access to more clinical records, some have expressed concern that having more access would change the standard of care applicable in the medical malpractice context.¹⁹ Attempts to analyze impact of electronic exchanges on potential liability are inconclusive,²⁰ and do not support eviscerating patient control. Thus providers need to work with patients, as they do currently, to secure consent to the PHI the provider needs to render effective care.

The ACLU is of the position that operational protocols (panel 5) should be developed that include, but are not limited to, the following:

- (1) require providers, prior to releasing patient names to the ILHIE, to advise each patient, individually, of the opportunity to be enrolled in the ILHIE, and of the right to consent to that enrollment (opt-in). A “Notice of Privacy Practices” letter or email, which effectively enrolls a person in the ILHIE, and which does not require specific consent to making one’s medical records accessible through the ILHIE, does not satisfy existing privacy policies or legal requirements.
- (2) advise patients that they have the right to segment parts of their personal health record, that the patient considers sensitive, e.g., records pertaining to intimate partner violence, that existing law specifically protects, e.g., substance abuse treatment at a federally-supported facility, or that receive other protections through law, such as constitutional restrictions on invading the zone of privacy around a woman’s decision to have an abortion;
- (3) require providers seeking to distribute or to request segmented sensitive health information to secure written consent from patients before distributing or accessing sensitive segmented health information;
- (4) require providers to tag, segment and sequester, any patient information that is protected by law from sharing in a way that personally identifies patients, as for example, records that identify individual women who have had abortions;
- (5) develop specific protocol for minors to allow the protection of the PHI identified in part D, below;
- (6) allow patients to revoke any consent provided, thereby restricting future sharing of such information; and,
- (7) develop protocol directing that communication about consent and segmentation be written and delivered in a manner that is easily understood, even to marginalized populations.

Several states already have adopted laws or regulations that afford patients the right to decide whether sensitive health information will be accessible through a state-wide registry. If Illinois adopts specific consent and segmentation requirements, sharing across state lines will be facilitated.

¹⁷ See, e.g., *Stanley v. Illinois*, 405 U.S. 645, 656 (1972); *Bowen v. Gilliard*, 483 U.S. 587, 629 (1987).

¹⁸ White Paper: Consumer Consent Options at 16.

¹⁹ *Id.* at 53-54.

²⁰ *Id.* at 54.

The ACLU also maintains that patients also must have the ability to restrict disclosure of PHI to payors. At a minimum, the Committee should recommend rules that:

- (1) consistent with the HITECH Amendments to HIPAA, allow patients to restrict disclosure to payors of PHI related to treatment or services for which the patient has paid out of pocket,²¹
- (2) consistent with the federal Genetic Information Non-Discrimination Act,²² and the Illinois Genetic Information Privacy Act,²³ allow a patient to restrict access to payors;
- (3) allow patients to restrict access to payors to all PHI except for that medical treatment or service for which reimbursement is being sought by the payor seeking access:

²¹ 42 U.S.C. § 17935, et seq., White Paper at 12. In order to comply with this provision, an exchange may need to develop a segmentation procedure by which a person's information could be exchanged for treatment but not payment or without operations.

²² 42 U.S.C. sec. 2000

²³ 410 ILCS 513

D. Special Considerations Pertaining To Minors.

Access to the health records of minors presents the ILHIE with additional legal complexities of consent and segmentation. Although parents are usually considered the “personal representatives” of minors for most purposes for dealing with access to PHI, both state and federal laws impose significant limitations on sharing minors’ PHI with parents. Thus, the ACLU takes the position that the Committee should recommend policies that require a minor’s specific consent before certain sensitive health records can be shared with personal representatives, including parents and guardians; and, that afford minors their right to segment and sequester certain health records. These requirements have constitutional and legal dimensions.

Under Illinois state law, minors who understand the risks, benefits and alternatives to certain health care services, are considered legally competent to give informed consent – **without parental knowledge or consent** – to the following health care services:

- (1) contraceptives and pregnancy testing;²⁴
- (2) emergency contraception;²⁵
- (3) testing, treatment and counseling for sexually transmitted diseases²⁶ (although providers are encouraged, where appropriate to involve a minor’s family in the minor’s treatment for a sexually transmitted disease, provider must first obtain minor’s consent);
- (4) HIV testing, treatment and counseling;²⁷
- (5) health services associated with criminal sexual assault or abuse;²⁸
- (6) abortion services;²⁹
- (7) substance abuse case;³⁰
- (8) Confidential mental health counseling or psychotherapy on an outpatient basis, albeit with certain limitations.³¹

HIPAA itself recognizes an exception to sharing PHI with a parent or personal health representative when state law allows a minor to consent to health care procedures and where the minor does in fact give consent.³²

²⁴ 325 ILCS 10/1 (1991).

²⁵ *Id.*; 410 ILCS 70/5(b) (2010).

²⁶ 410 ILCS 210/4 (1995), Ill. Admin. Code tit. 77, § 693.130.

²⁷ 410 ILCS 210/4, Ill. Admin. Code tit. 77, § 697.420 (providers encouraged but not obligated to notify minor’s parent of positive test result).

²⁸ 410 ILCS 70/5(b); 410 ILCS 70(1); 720 ILCS 5/12-15 (2011) (definition of criminal sexual assault includes criminal sexual abuse); 410 ILCS 210/3(b), Ill. Admin. Code tit. 77, § 545.60(f).

²⁹ *Hope Clinic v. Adams*, No. 09-CH-38661, Temporary Restraining Order (Cir.Ct. Ill. Nov. 4, 2009).

³⁰ 410 ILCS 210/4.

³¹ 405 ILCS 5/3-501(a) (1989), 740 ILCS 110/4(a)(3) (2010)

³² See 45 C.F.R. § 164.502(g)(3)(i)(a); see also White Paper: Data Segmentation at 14-15.

Some states already have incorporated limits on the access a personal representative will have to a minor's records. New York has decided that health records of a minor above a certain age should be excluded from the exchange, but that the records of minors below that age can be included.³³ Similarly, Kaiser's Mid-Atlantic region of providers limits the information in the health records of 13 to 18 year olds to allergies and immunizations.³⁴

This Committee should recommend protocol that requires all data systems contributing to the exchange to:

- (1) tag all data related to a procedure to which a minor has self-consented;
- (2) record that data in a structured field; and,
- (3) then to exclude that data from the registry unless the minor specifically has been afforded a confidential opportunity to consent to the inclusion of that data in the registry and a specific opportunity to segment it from disclosure to a personal representative, including parents.

III. Protect the Right of Patients to Confirm or Correct the Accuracy of Their Electronic Health Records.

Illinois and federal law allow patients to access their medical records that are held by individual providers.³⁵ Current law also entitles patients to request amendments to their health records.³⁶ Commensurate with its other recommendations, the ACLU believes this Committee should recommend a patient-access policy that complies with this existing law. To ensure that patients can access and request amendments to their health records, this Committee should recommend that HIE entities develop concrete plans to give patients electronic access to their compiled individually identifiable health information and develop clearly defined processes (1) for individuals to request corrections to their health information and (2) to resolve disputes about information accuracy and document when requests are denied.³⁷ Additionally, this Committee should recommend policies that require individuals and entities to take reasonable steps to ensure that an individual's health information is complete, accurate, and up-to-date. As such, it should also recommend that a correction or amendment is automatically sent to any provider who has accessed the patient's medical records through an HIE.

Incorrect information can have devastating impact on a patient's care. If patients do not retain the rights to get and amend that they currently have, inaccuracies can lead to problems with a patient's employment, insurance, or follow-up care. Whereas in the current paper file system, if a patient sees an inaccuracy, he need only correct one doctor's file. But an HIE augments the impact of any error because errors can rapidly transmit from one provider to another. Accordingly, patients should retain the ability to correct or amend their medical records.

IV. Patient Data Should Be Protected by Prohibiting the Sale of Data and Sanctioning the Misuse of Medical Information.

³³ White Paper: Data Segmentation at 37-38.

³⁴ *Id.* at 38.

³⁵ Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, § 261-264; 735 ILCS 5/8-2001(b); *Clay v. Little County of Mary Hospital*, 277 Ill. App. 3d 175 (1st Dist. 1995).

³⁶ HIPAA, P.L. 104-191; United States Department of Health and Human Services, *OCR Privacy Brief: Summary of the HIPAA Privacy Rule*, 2003.

³⁷ Department of Health and Human Services, *Program Information Notice: Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program*, Document Number ONC-HIE-PIN-003, 5-6.

Consumer confidence sits at the core of medical record privacy protections. Without a consumer's trust that her medical records will be safe, she may not seek certain treatment or disclose certain information.³⁸ Although most providers and other entities accessing PHI clearly respect patient autonomy and privacy, this Committee should recommend policies to protect against those few who would misuse patient records. Those policies should clearly define what constitutes misuse and should and impose sanctions should such misuse does occur.

At a minimum, misuse should be defined to include accessing records for individuals with whom the provider, payor, or other entity accessing PHI does not have a professional relationship, such as viewing the records of a celebrity. Misuse also should include selling personal health information, using personal health information to target individuals or providers for promotional pitches or advertising campaigns, redisclosing personal health information or profiting from its sale. Misuse also should be defined to include using personal health information to discriminate against, mistreat or withhold treatment from patients.³⁹ These protections are grounded in Illinois and federal laws that recognize the danger of disclosing information that should be confidential.⁴⁰ In addition to breaching patient confidence, any type of misuse could have public health consequences.⁴¹

Because of the potential for misuse and the associated consequences, the Committee should also recommend a policy that mitigates and sanctions such misuse. For example, reasonable mitigation strategies should be established and implemented as appropriate, including notice to individuals of privacy violations and security breaches.⁴² The ILHIE Authority should also conduct audits to ensure compliance with these security precautions, and should retain the authority to revoke the privileges of providers who misuse the exchange.

In a world with advancing technology and ease of remote information access, this Committee also should require HIE entities to ensure that appropriate monitoring mechanisms are in place to report and mitigate non-adherence to policies and breaches. It should also recommend policies that focus on detecting, preventing, and mitigating any unauthorized changes to, or deletions of, individually identifiable health information.⁴³ For example, individual health information should be protected with reasonable administrative, technical and physical safeguards to ensure its confidentiality, integrity and available and to prevent unauthorized or inappropriate access, use or disclosure.⁴⁴ It should be encrypted, and require authentication and authorization, and the ILHIE Authority should retain the ability to revoke the privileges of providers who misuse it.⁴⁵ Further, patients should have the ability to obtain reports of the health information that has been shared through the exchange, the identities of those who have accessed their information, and security breaches.⁴⁶

³⁸ See, e.g., 410 ILCS 305/2(2).

³⁹ NYCLU, *Protecting Patient Privacy: Strategies for Regulating Electronic Health Records Exchange*, March 2012, 22.

⁴⁰ See, e.g., 42 C.F.R part 2; 410 ILCS 305/2; 410 ILCS 513/1; 740 ILCS 110/1.

⁴¹ 410 ILCS 305/2(2).

⁴² Department of Health and Human Services, *Program Information Notice: Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program* at 9.

⁴³ *Id.* at 8.

⁴⁴ *Id.* at 8-9.

⁴⁵ White Paper: Consumer Consent Options at 21-22.

⁴⁶ R.I. Gen. Laws § 5.37-10 (2009).

V. Conclusion: Privacy Protections Yield Better Care, More Patient Engagement, and Ultimately, More Participation in Electronic Health Information Exchanges.

Numerous polls show that patients express strong support for the implementation of electronic health records; patients appreciate the potential benefits of electronic health records. However, those same studies reveal significant patient concern about who has access to their health information and how that information is used.⁴⁷ As The George Washington University White Papers on Consumer Consent and Data Segmentation recognize, numerous policy objectives that will be advanced by devising a HIE that protects patient privacy and security. In addition to the significant legal considerations detailed above, enabling patient preference enables greater patient autonomy, facilitates greater patient engagement in their own health care, and builds greater patient trust in the system, thus encouraging greater participation in the exchange and producing greater public health benefits⁴⁸

⁴⁷ White Paper: Consumer Consent Options at 24-25.

⁴⁸ White Paper: Data Segmentation at 1-31.