

## **NJHIT POLICY COMMITTEE – REPORT OUT ON**

### **APRIL 12, 2010 MEETING RE: NEW JERSEY PRIVACY & SECURITY FRAMEWORK**

*Prepared by:* Jed Seltzer and Helen Oscislawski

*Submitted by:* Al Gutierrez, HITC Policy Committee

May 6, 2010

#### **I. OBJECTIVES**

On April 12, 2010, the NJHIT Policy Committee convened a public meeting to discuss issues, challenges, and potential solutions to barriers posed by **state laws** governing **access, use** and **disclosure of health information**, and their affect on electronic health information exchange (HIE) through a New Jersey regional health information organization (RHIO). The meeting was open to the public. In addition, in order to maximize on the breadth of experience represented at the meeting, the Policy Committee specifically invited individuals with privacy compliance experience, including, among others, privacy officers, consultants, and attorneys who regularly work with privacy laws.

The primary objective of the meeting was to elicit information from New Jersey health care providers, facilities and other stakeholders regarding the following:

- What sorts of **privacy practices** have New Jersey health care providers implemented, and are any of these viewed as potential barriers to participating in electronic HIE or a RHIO?
- Are there specific **state laws** that are viewed as insurmountable barriers to HIE?
- Are there prevailing views/concerns with patients' choice to **opt-in** or **opt-out** of HIE in NJ?
- What **solutions** have been implemented for HIE within current NJ privacy law framework?
- What sort of **legislation** would be desirable/ helpful to support multi-stakeholder HIE in NJ?
- What steps should be taken to ensure **patients trust** and full engagement of the NJ RHIO?

#### **II. FEDERAL BACKDROP**

It should almost go without saying that the federal government has fully committed to transitioning the health care sector towards utilizing electronic health records (EHRs) and linking separate silos of health information through interoperable technology. This commitment is evidenced by everything from the allocation of billions of federal dollars towards HIE, RHIOs and education, to the promulgation of regulations (e.g., meaningful use) that include required elements of data exchange, to the numerous pro-HIE public policy statements being issued by the Office of National Coordinator (ONC). Indeed, there is mounting expectation if not distinctly palpable pressure on health care providers to implement EHRs and connect to networks and/or RHIOs so that we can quickly “realize” potential improvements in efficiency and quality of care through electronic HIE . However, lest we become too zealous or careless with how patient information is exchanged, the pro-privacy voice is loud and clear.

For instance, the **HIT Policy Committee** was established within ONC and is charged with making recommendations to the National Coordinator on a policy framework for the development and adoption of a nationwide health information infrastructure (NHIN), including standards for the exchange of patient medical information. The Privacy & Security Policy Workgroup of the HIT Policy Committee

specifically works to address privacy and security in the HIT policy context, and is looking to define and address the policy challenges related to privacy and security; set principles around privacy and security; and suggest various methods of ensuring privacy and security. Between ONC, the HIT Policy Committee and other federal agencies such as CMS, helpful resources, guidance and whitepapers are now available to the public for reference on important privacy issues, such as consumer consent (e.g., opt-in versus opt-out), the impact of CLIA on patient-access to their data, authentication and audit best practices, among others. In addition to such federally-formed committees, public watchdog groups, like Dr. Deborah Peel's organization "Patient Privacy Rights," powerfully inject a pro-privacy/pro-patient-control viewpoint into the debate and work incessantly to ensure that patient privacy does not take a back seat on the HIE train.

However, as both government and private groups work to try and strike the "proper" balance between electronic HIE and patients' right to confidentiality and control over their information, New Jersey's quickly burgeoning HIE communities and the State RHIO are left holding the state privacy law bag. Our challenges include trying to understand how our State's privacy laws differ from the federal privacy "floor," what standards (federal or state) should be followed, and whether certain "outdated" State laws need to be revised or new legislation needs to be enacted in order to fit and properly address the changing landscape. Moreover, at least for purpose of developing a State-wide RHIO, all such State laws must be fully vetted from a private sector and government sector standpoint.

### **III. NEW JERSEY'S PRIVACY & SECURITY LAWS**

New Jersey does not have a broad sweeping health information privacy law, rather patients' privacy rights are addressed through a **patchwork of statutes and regulations**. Generally, with a few exceptions, these laws can be grouped or categorized as follows:

- **Facility-specific** laws (e.g., licensed hospitals; ACFs; SNFs; pharmacies; clinical labs etc.)
- **Provider-specific** laws (e.g., licensed physicians; nurses; pharmacists; psychologists etc.)
- **Sensitive Information** laws (e.g., HIV/AIDS; Genetic Information; STDs; Drug Rehab)
- **Government Program**-specific laws (e.g., Medicaid; Family Planning; Prisons; FQHCs etc.)

Within the forgoing categories, one will find New Jersey statutes, regulations and even case law that governs or effects how health information can be used and disclosed. For instance, regulations governing New Jersey licensed acute care hospitals state:

*"Every New Jersey hospital patient shall have the following rights, none of which shall be abridged by the hospital or any of its staff . . . 21. To confidential treatment of information about the patient. Information in the patient's records shall not be released to anyone outside the hospital without the patient's approval, unless another health care facility to which the patient was transferred requires the information, or unless the release of the information is required and permitted by law, a third party payment contract, a medical peer review, or the New Jersey State Department of Health." N.J.A.C. 8:43G-4.1(a)21.*

Regulations governing New Jersey licensed ambulatory care facilities (ACF) contains a provision almost identical to the one set forth above, however the ACF rules add the following:

*"The facility shall establish and implement written policies and procedures regarding medical records including, but not limited to,*

*policies and procedures for the following: 1. The protection of **medical record information** against loss, tampering, alteration, destruction, or unauthorized use. The patient's **written consent shall be obtained for release of medical record information**; 2. The specific period of time, not to exceed 30 days, within which the medical record shall be completed following treatment or discharge; and 3. The transfer of patient information when the patient is transferred to another health care facility, or if the patient has been an inpatient and becomes an outpatient at the same facility, to ensure continuity of care.” N.J.A.C. 8:43A-13.5(a). “*

A quick look at the Board of Medical Examiner (BME) regulations governing New Jersey licensed medical practitioners reveals yet even further differing standards:

*“Licensees shall maintain the confidentiality of professional treatment records, except that: 3. The licensee, in the exercise of professional judgment and in the **best interests of the patient** (even absent the patient's request), **may release pertinent information about the patient's treatment to another licensed health care professional who is providing or has been asked to provide treatment to the patient, or whose expertise may assist the licensee in his or her rendition of professional services.**” N.J.A.C. 13:35-6.5(d)3.*

However, if the foregoing provides practitioners with somewhat broader discretion to share information in connection with treatment of a patient, the provision that follows it imposes a separate more cumbersome administrative requirement if the patient *initiates* the request for release of his/her “treatment record”:

*“Where the patient has requested the release of a professional treatment record or a portion thereof to a specified individual or entity, in order to protect the confidentiality of the records, the licensee shall: **1. Secure and maintain a current written authorization**, bearing the signature of the patient or an authorized representative; 2. Assure that the scope of the release is consistent with the request; and 3. Forward the records to the attention of the specific individual identified or mark the material “Confidential.” N.J.A.C. 13:35-6.5(e).*

The foregoing offers just a glimpse of the variations in standards that exists under New Jersey’s current patchwork of confidentiality laws, and which can require different procedures to be implemented for the use and disclosure of patient health information depending *what type* of Facility-specific or Provider-specific rules applies. Add to this still other New Jersey laws governing specific categories such as minors seeking emancipated treatment, who is a “legally authorized” representative under state law, patient access-rights and timeframes, Sensitive Information laws, as well random standards peppered here-and-there on topics such as digital signatures, and the challenge of implementing consistent privacy standards for electronic HIE between various New Jersey providers – even just hospitals and physicians – becomes compounded. In *some* cases, statutory and regulatory language may be *interpreted* to possibly allow providers to engage in electronic HIE for treatment consistent with the black letter of the law and without having to implement unnecessarily cumbersome administrative procedures; however, in other instances, it simply cannot.

Thus, the State of New Jersey may be at a crossroad, and as such, the **Policy Committee is recommending that the State, its various licensing authorities (e.g., DHSS; DHS; BME etc.) and our State Legislature consider and respond to several crucial questions:**

- ***Does New Jersey's current patchwork of health information privacy laws adequately support and further the State's (and federal government's) desire to connect providers for engaging in electronic HIE through a RHIO?***
- ***Have the differing standards embedded in various State statutes and regulations become outdated and misaligned with a national and state movement from paper medical records to electronic health records, and towards electronic HIE?***
- ***Could state legislation be introduced to better define and support the State's policies and remove any unnecessary barriers with regard to electronic HIE for appropriate purposes (e.g., treatment)?***

#### **IV. BREAKING DOWN THE BARRIERS**

On November 12, 2009, ONC's National Coordinator, Dr. David Blumenthal, issued a "Message" to the public which expressly states that ***"barriers to exchange of health information must be broken down."*** More specifically, the Message from Dr. Blumenthal states that the HITECH Act works to eliminate inappropriate barriers to electronic HIE as follows:

- ***It squarely tackles the commercial barriers.*** The HITECH Act calls for the "development of a nationwide health information technology infrastructure that allows for the electronic use and exchange of information and that ... promotes a more effective marketplace, greater competition (and) increased consumer choice," among other goals (Section 3001(b)). This means **we cannot support arrangements that restrict the secure, private exchange of information required for patient care across provider or network boundaries.**
- ***It tackles the technical barriers.*** The HITECH Act focuses on "interoperability" or "interoperable products." In plain English, this means that our **policies, programs and incentives must aim for electronic health record (EHR) software and systems that can share information with different EHRs and networks so that information can follow patients wherever they go and to build the pipelines to carry this information.**
- ***It provides building blocks for information exchange across jurisdictions.*** The grants for states and state-designated entities in Section 3013 – which will total \$564 million – target information exchange across boundaries, not only within each state but explicitly as part of a nationwide framework. We will start announcing the awards this winter. These **grantees' activities must support interoperability that lets patient data follow the patient across political and geographic boundaries.**

Through its successful ARRA grant application, a number of New Jersey's largest HIE efforts have qualified to receive a total of \$11 Million dollars from the federal government to be used towards developing the necessary infrastructure to allow health care providers to exchange patient information for the purpose of treating patients. Thus, these New Jersey HIEs are not only expected but may now also, as stated by Dr. Blumenthal in his Message, be **required** to develop mechanisms to allow for patients' health information to follow the patient beyond the 4-walls of one facility as needed by practitioners to treat their patients. Nevertheless, the right balance with confidentiality and patient control must still be struck.

Towards the end of his Message to the public, Dr. Blumenthal correctly notes:

*“If we are to reap the benefit of information exchange, Americans must also be assured that the most advanced technology and proven business practices will be employed to secure the privacy and security of their personal health information, both within and across electronic systems, and that **persons and organizations who hold personal health data are trustworthy custodians of the information.** We must have comprehensive, clear and sustainable policies that strengthen existing protections, fill gaps as they emerge, fortify new opportunities for patients' access to and control of their information and align with evolving technologies.”*

Therefore, if adequate patient-control is not afforded, individuals could flee the NJ RHIO despite our best efforts; however if state law requirements cannot be implemented in a reasonable manner that do not otherwise paralyze the health care delivery system with administrative procedures, electronic HIE could fail for this State. Thus it is imperative for New Jersey to determine what the “correct” balance should be.

## **V. NEXT STEPS AND RECOMMENDATIONS FROM THE POLICY COMMITTEE**

The meeting held on April 12, 2010 produced robust discussion. Topics discussed and comments made include: (i) whether there is a preference that the State adopt an “opt-in” or “opt-out” of HIE policy; (ii) whether certain state law requirements enacted in a “paper medical record” world era may no longer be applicable to evolving practices in an electronic age; (iii) whether past analyses of state laws can be leveraged to produce a current updated review of state law; (iv) would enactment of a state-wide statute be beneficial for addressing differing state standards pertaining to health information exchange and access, or should the authority already vested in certain State Departments (e.g., DHSS; DOBI; DHS) be utilized to amend current disparate standards.

The following main ideas and initial recommendations resulted:

1. The attending audience was in support of New Jersey adopting an **“OPT-OUT” approach** to electronic HIE in this state (meaning that patient data is in the exchange, with proper consent, unless the patient chooses to opt-out) including in connection with the New Jersey RHIO. Further decisions will be needed regarding the granularity of any State-mandated right to opt-out – e.g., Is it all or nothing (you are in the RHIO or you are out)?; Can patients opt-out of certain HIE/RHIO participating *Providers? Facilities? Episodes of care? Information?*
2. Comprehensive **legislation** or regulation may be needed to update State laws to better enable electronic HIE between private facilities and statewide through the RHIO. Such legislation would address the at least the following key elements:
  - a. Access to information through the exchange for use by physicians and other health-care providers will be limited to **providers authorized** to see data on certain patients that they are **treating**;
  - b. Aggregated, de-identified data may be accessed by the Department of Health and Senior Services, the Department of Human Services, the Department of Banking and

Insurance, the Department of Children and Families, and any departments and agencies with their statutory authority;

- c. When consenting to the release of data at the point of care, patients are opted into the exchange, except certain circumstances and types of sensitive data (e.g., HIV, genetic information, venereal disease, others) will always be behind a “break glass” requiring a higher level of “proof” of authority to access such information;
  - d. Patients/consumers will have a standard right to access the data about them that resides in the RHIO when they request it;
  - e. Any state laws or requirements that conflict with the enacted legislation would be amended by the new legislation;
  - f. Further language would be inserted regarding the permissibility or prohibitions on secondary uses [to be defined] of information in the RHIO;
  - g. Requirements related to breach notification through multiple HIE participants should be consistent with HITECH and HHS regulations;
  - h. Some type of limited immunity should be granted to providers who are producers of data insofar as they are not responsible for any future decisions made by providers who treat the patients in question.
3. Each regional HIE, and the NJ RHIO, must develop **security standards** that will ensure adequate privacy consistent with HIPAA and HITECH, according to emerging security standards from NIST/HITSP/NHIN, and each new entrant into an HIE must undergo a screening process to ensure the security in their systems meet the RHIO thresholds.
  4. In so far as it will be necessary to fully understand each and every legal barrier currently existing in State law in order to propose amending language, then the Commission should evaluate whether a RFP process can be employed to engage a law firm to do a formal and written crosswalk between federal law and existing state law, and between various state laws governing different types of health-care institutions and data, so as to identify any barriers to the exchange of information and any inconsistencies between State law and the new 'HITECH' law. The NJHIT Commission should first identify all prior efforts that have already been completed and any such state law preemption analysis that exist – e.g., through HISPC; Medicaid; NJHSS etc. Any such work products should be consolidated and made accessible at a single-point location (e.g., NJHITC website), and should be leveraged for further state law review and final determinations.
  5. There must be a State-level multi-disciplinary governing entity entrusted with the **oversight** of the privacy and security of the data in a Statewide RHIO, and that entity must include clinical, policy, and technological expertise. This governing requirement may possibly also be extended to oversee certain activities of regional HIEs.