



January 3, 2008

Re: Proposed Legislation regarding a state-wide HIE

Dear Colleagues:

The R.I. Affiliate of the ACLU has participated in RIQI Policy & Legal Committee meetings regarding the development of a state-wide Health Information Exchange (HIE) over the last two years. However, due to significant unresolved concerns about confidentiality and privacy, as embodied in the group's proposed legislation, we are no longer be able to do so.

Our decision to no longer participate in the group's discussions was not made lightly. Our Board of Directors discussed this at great length at a recent meeting, but concluded that, since we will almost certainly be in the position of actively opposing the legislation, we did not want to be formally criticizing it while remaining an active member of the group supporting it (and responsible for drafting it). We felt this would put both our organization and the Policy and Legal Committee in a difficult position.

In order to help you understand why we came to this decision, we wanted to share with you some of our major objections to the legislation. For the most part, these are objections, we would note, that we have raised previously but without successful resolution.

We recognize the medical treatment benefits that can result from the use of a system of electronic health information exchange, but we also believe the proposed legislation does not provide an adequate privacy framework for any such information exchange.<sup>1</sup> Our primary concerns are as follows.

---

<sup>1</sup> Serious privacy concerns have been expressed by the Government Accounting Office (GAO) regarding national efforts to coordinate the development of similar electronic health information nationwide. In April 2004, President Bush charged the U.S. Department of Health and Human Services (HHS) with developing and executing a plan for a nationwide system for electronic health information exchange within 10 years. HHS' Office of the National Coordinator for Health Information Technology awarded over \$42 million in contracts to advance that goal in 2005. In January 2007, the GAO released a report (GAO-07-238) in response to Congress' request, which was critical of HHS' efforts to ensure that privacy protection was part of its overall national health information technology strategy. The GAO noted that

1. There is insufficient state control over the HIE, so that important privacy and security concerns will be determined by private entities.

The proposed legislation lacks specificity with regard to security measures and patient rights and leaves much decision-making in the hands of private entities. It requires very little state oversight of HIE policy and practice. Although the Executive Office of Health and Human Services (or its designee) is authorized to issue regulations, it is only required to do so in very limited circumstances:

- To establish the “HIE Advisory Commission,” that will be responsible for making recommendations regarding how confidential health care information stored in the HIE can be used;
- To define the process for patient and provider choice to participate in the HIE;
- To define the process whereby the HIE will authenticate recipients to whom it discloses confidential health care information; and
- To define the process for patients to terminate participation in the HIE.

As its name indicates, the HIE Advisory Commission established by the legislation is advisory only, and will have no formal power in deciding issues regarding confidentiality. Further, there is no requirement for state regulation of the private Rhode Island Health Information Organization (RHIO), which is responsible for all administrative, operational and financial functions of the HIE. The RHIO, not the state, will develop and enforce policies for receiving, retaining, safeguarding and disclosing confidential health care information in the HIE. The RHIO’s responsibilities will be established by contract with the state. The state will thus have a very limited ability to act quickly to resolve any disputes about the policies and practices that the RHIO establishes for the HIE. It is also not clear how the RHIO will be able to effectively “enforce” any policies regarding security or privacy that it establishes for the HIE.

The proposed legislation does require the HIE to have *some* security procedures. In particular, the HIE generally must: “authenticate” persons who seek information from the HIE according to procedures created by the state agency regulation; limit access to health care information to persons having a “need to know” that information; identify the person who has responsibility for maintaining security procedures for the HIE; provide statements to employees about the need for confidentiality and penalties for violation of the requirements of the HIE legislation; and not retaliate against employees or agents for whistleblowing. However, the details of how these security measures will be operationalized are not provided, and these provisions are too limited, from our perspective, to ensure the privacy and confidentiality protections that we consider essential for a database of this kind.

---

HIPAA did not adequately protect the privacy of information stored in an HIE, and that state laws vary greatly in their applicability to an HIE. The GAO report concluded that HHS did not have an overall approach for addressing key privacy principles. Those principles included ensuring that (1) only the minimum amount of information necessary is disclosed to only those entities authorized to receive it; (2) individuals retain the right to access and amend their own health care information; and (3) adequate security and privacy measure for confidential health care information are implemented.

2. The legislation does not adequately address third party access to an individual's confidential health care information stored within the HIE.

The legislation generally requires providers and others to obtain consent prior to accessing an individual's information stored within the HIE, but lists three exceptions to the requirement for consent. A person's health care information could be accessed by: (1) a health care provider in an "emergency" for diagnosis or treatment; (2) the Department of Health and other public health authorities, pursuant to their responsibilities under state and federal law; and (3) the RHIO for the operation and oversight of the HIE.

In addition to these three explicit provisions for access without consent, the legislation creates the opportunity for a person's health care information to be used in ways not related to an individual health care treatment.

- Once a health care provider is given permission to access a person's health care information in the HIE, that provider will have access to *all* of the person's information. In addition, the provider can use and disclose that information for any purpose currently allowed by state or federal law, including the 24 exceptions under the Confidentiality of Health Care Communications and Information Act. For example, the provider could use or disclose the information for the purpose of conducting scientific research, or whenever the provider thought the information was necessary to obtain adequate legal representation.
- Although the legislation attempts to prevent confidential health care information from being accessed from the HIE pursuant to a subpoena, this protection is, in all likelihood, illusory. This limitation is likely to be quickly challenged in court. Because successive R.I. Supreme Court cases have severely limited, as a constitutional matter, the ability of individuals to keep their confidential health care information out of court proceedings, there is a very strong chance that the Court will find that these statutory efforts to restrict the authority to subpoena information from the HIE cannot stand. As a result, it is probable that attorneys in a wide variety of cases – contested divorces or other family disputes, for example – will be able to easily obtain medical records of providers that the lawyer had no idea even existed.
- The legislation does not attempt to prevent third parties, such as employers, insurers and financial institutions, from obtaining "nominal consent" in order to access an individual's confidential health care information from the HIE.

As suggested above, there is no limit on the kind or amount of information that can be disclosed in response to a request for access. HIPAA requires that covered entities have policies to ensure that they disclose only the "minimum necessary information" about a person's health care, except for treatment uses and the health care entity's operations. There is no provision in the proposed legislation requiring that the HIE disclose only the "minimum necessary information" in any context. This may be particularly important in the context of 3<sup>rd</sup> party use and access to a person's health care information within the HIE.

3. The proposed legislation does not adequately protect a person's "choice" to not participate in the HIE.

The proposed legislation does not address whether an individual will have to affirmatively agree to participation (opt-in), or will just be given the chance to object to participation (opt-out). Apparently, the state will determine by regulation whether to use an opt-in or opt-out approach.

The legislation envisions that other persons may be able to decide whether a person will participate in the HIE. These persons include not only those already recognized in Rhode Island as substitute decision-makers, such as an agent under a Durable Health Care Power of Attorney or a guardian with authority to make health care decisions, but also a new category of substitute decision-maker – “another legally appropriate decision-maker.” The latter is authorized to consent to the participation of a “decisionally impaired” person, if a guardian, conservator, or health care agent is not “available.” It is not clear who will decide what “unavailable” or “decisionally impaired” means.

More significantly, the HIE is premised on an “all or nothing” approach to participation and information-sharing. That is, a participating patient is unable to exclude from the HIE *any* medical information, including information that has historically been given heightened legal protection – such as records of genetic testing, sexually transmitted diseases, mental health treatment, and alcohol or drug treatment. By the same token, any person entitled to access information in the HIE about a patient may be privy to the entire record of the client, including these sensitive records.

Finally, the legislation does not ensure that a person who decides not to participate in the HIE will still be able to access health care. If a person has concerns about particular kinds of information that will be in the HIE, and potentially accessed by all treatment providers as well as 3<sup>rd</sup> parties, he or she may well decide not to participate in the HIE. However, there is nothing in the proposed law that prohibits health care providers from refusing to accept as a patient a person who does not participate in the HIE. Thus the “choice” not to participate may become illusory.<sup>2</sup>

4. The legislation does not provide explicit rights and remedies for individuals who dispute the accuracy of the information within the HIE or how health care information was used or disclosed by the HIE.

There is no process provided for a person to request the HIE to amend his or her personal health care information. The person's only recourse will be to make a request to amend

---

<sup>2</sup> The patient authorization form mailed to the Policy and Legal Committee on November 16, 2007 reflects the proposal's ambiguity regarding “choice.” The “opt-out” language is entitled “*Refusal to Participate*,” – a term that belies the voluntariness of participation. The same paragraph also indicates that the HIE will be storing a person's information, regardless of their agreement to participate. The form further confirms the breadth of records access allowed by the bill, as the consenting patient, by signing the waiver, is acknowledging that confidential health care information can be released not only for purposes of treatment and coordination of health care, but also for “health care operations and disease management programs.”

information to a participating provider. Even in that instance, there is no requirement that the request be acted upon, and no process specified for resolution of disagreement about amendment. (Some providers may be subject to HIPAA's procedures for resolving disputes about the accuracy of an individual's health care information.) Even if a provider agrees to amendment, the legislation does not require correction of health care information stored within the HIE. There is also no process in place to correct errors that may have been made by the HIE itself and not a provider, such as matching errors or data entry errors.

The proposed legislation requires that persons be notified of any breach of the security system of the HIE, pursuant to the procedures under the Rhode Island Identity Theft Protection Act. However, it is not clear whether information stored in the HIE will be subject to the Identity Theft Protection Act, since that law only applies to *unencrypted* personal information that either has a SSN or driver's license number associated with it.

We hope this non-exhaustive summary helps explain why we have come to the position we have in bowing out of the committee's deliberations. We would point out that, back in March of this year, we sent an e-mail to members of the group, raising many of the same concerns that are addressed in this letter. The fact that so few of them have been favorably addressed gives us pause.

Experience teaches that if basic privacy and confidentiality issues are not adequately addressed up-front, the issues regarding patients' privacy rights will be decided by default – and almost certainly on the basis of other priorities. In too many instances, we believe, important confidentiality issues referred to the group's technology committee have been deemed infeasible. This, we believe, puts things upside down. The technology should be accommodating patients' legitimate privacy interests, not the other way around.

We want to emphasize that we appreciate the opportunity we have had to provide input to this process, and we remain available to review concerns. We expect that we will be working with group members as the legislative process unfolds, and in doing so, we hope to better ensure that privacy policies and practices are embedded within the framework of the HIE.

Sincerely,

Steven Brown  
Executive Director

Anne Mulready  
Board of Directors