COMMENTS CONCERNING RULES AND REGULATIONS PERTAINING TO THE RHODE ISLAND ALL-PAYER CLAIMS DATABASE

November 5, 2012

The RI ACLU is concerned with a number of provisions in these proposed regulations which could severely impact the privacy of Rhode Island's patients. Certain portions of these regulations seem to be in tension not only with the federal HIPAA law, but with the very statute which guides this database's creation. In addition, the regulations sacrifice both the privacy of patients and the rights of those interested in receiving data, while creating an unnecessarily burdensome system for encoding and storing information.

Before we address some of the more complex issues in the regulations, we wish to bring attention to a few items which are missing from these regulations.

First, the regulations appear to exclude long-term care insurance providers from the list of those exempted from the requirements of the all-payer claims database, although these providers are specifically exempt under R.I.G.L. §23-17.17-9. We believe this to be an oversight which can and should be easily rectified.

Second, and of far greater concern, is the removal of any mention in the current proposed regulations of "indirect personal identifiers." At the community review meeting in February of this year, the draft regulations at that time included a definition of indirect personal identifiers which included patient information that "a person with appropriate knowledge of and expertise with generally accepted statistical and scientific principles and methods" could use to uncover

individually identifiable information. These indirect personal identifiers were included in the definition of "personally identifiable information," thereby prohibiting the transmission or use of such identifiers and adding a critical layer of protection for patients' medical privacy. Through this language, the Department recognized the need to protect not only overt personal identifiers, but also that data which any individual with the right training, including researchers and statisticians who may seek access to much of the information contained within this database (or those reviewing the results of any such research), could use to uncover personal information.

The decision by the Department to remove this definition is troubling, as it potentially sanctions the recovery of medical information that could be traced to individuals, and greatly increases the likelihood that a patients' private information may be uncovered. While the Department previously made an effort to protect patient privacy in this regard, these regulations appear to abandon those efforts for no discernible reason. The attempt in this proposal to now address this issue is, we submit, feeble and ultimately useless. Section 7.3(d)(8) states that restricted release data "shall not be combined with any other available data source" that could potentially re-identify a patient. But we cannot conceive how, either legally or practically, the Department can prevent somebody from doing this. In essence, it is telling individuals they cannot make use of publicly available information. The Department has no authority to set such a restriction, which is why it is so important that limits be placed up front, on both the information that is collected and the information that is deemed public and restricted in the first place – not by attempting to prohibit the use of information after the fact. (In a similar vein, Section 7.3(i) of the proposal requires, as one consideration in whether to release restricted data, whether other data could be used to re-identify patients. But this should not be a "consideration" – it should be an absolute bar. The fact that the review process recognizes this scenario as a possibility is yet

another reason why a bar on the transmission of indirect personal identifiers should be addressed up front.)

Looking at the language under consideration at this time, we are particularly concerned with language appearing on page 12, discussing the release of "unavailable data elements." This term is not specifically defined by the regulations, and it is unclear whether it refers to personally-identifiable information or other confidential data submitted to the encryption vendor. Yet this paragraph specifically notes that data not considered public use or restricted release data is not to be used "outside of the Department *or other state agencies*." While the regulations further discuss the request and use of restricted release data by other state agencies, this paragraph appears to allow state agencies access to information beyond that which is permitted for public or restricted use. We can think of no reason for state agencies beyond the Department of Health to have access to data outside of that designated for public or restricted use, and are concerned with the apparent opening of this private information to other state agencies. This section should be altered to clarify that other state agencies outside of the Department can receive only public use or restricted release data. Indeed, depending upon the information that this paragraph is referring to, the Department itself may not even be entitled to this information in light of the statutory restrictions imposed on the Director being able to obtain personally identifiable data, which is itself acknowledged in Section 3.2 of the proposal.

This language further enforces concerns that the information contained within this database could be combined with other future databases for other purposes; nothing contained within the regulations prevents this from happening. If such data sharing, even of de-identified data, were to occur, it would become more and more likely that individuals with access to the data would be able to use the data to make personal identifications, especially if indirect personal

identifiers are stored within the system. In fact, there was testimony to that effect at the community hearing. In addition to restoring restrictions on the disclosure of indirect personal identifiers, the regulations should, at the very least, prohibit the state from combining the APCD with other databases in the future.

Throughout these regulations, strong protection must be ensured for the private identifying and medical information of Rhode Island's residents. Yet, on multiple occasions, the proposed regulations appear to minimize the protection of individually-identifiable information. This is most obvious in the discrepancy between "direct personal identifiers" as defined in the regulations, and "personal health information" as defined under the federal HIPAA law. While HIPAA identifies eighteen separate categories of protected information, the regulations under consideration exclude a number of these categories from protection. For example, HIPAA restricts the disclosure of "all elements of dates (except year) for dates directly related to an individual"; these regulations make no such protections. Additionally, HIPAA requires entities to protect information regarding account numbers, device identifiers, and "any other unique identifying number code," matters on which these regulations are silent. By differing from the HIPAA definitions in their identification of personally identifiable information, these regulations may be requiring health care companies to disclose more information than they are permitted under federal law. This was certainly not the intent of the General Assembly, as R.I.G.L. §23-17.17-11 clearly states data shall be available "to the extent allowed by HIPAA and other applicable law."

Additionally, state law specifies that information contained within this database "shall be transmitted in accordance with the rules adopted in HIPAA." Yet, disturbingly, the regulations themselves are relatively silent on the specific means and methods of information transfer in and

out of this database, beyond the information request procedures detailed for researchers and other interested parties. The regulations do, on several occasions, refer to an RIAPCD Technical Specification Manual, which does not yet appear to exist. As such, "provider file" has yet to be defined, the format of health care data sets has yet to be determined, and the code source and file specifications are yet to be released. Moreover, the regulations state the Director may require insurers to submit and update product information, as noted in the Technical Specification Manual. In order to protect the privacy of sensitive medical information, and ensure both compliance with HIPAA standards and the ability of providers to fluidly adopt any specifications detailed in the manual, these requirements, the resolution of these important issues should be publicly promulgated through an administrative rule-making process like this one, and not hidden in a forthcoming manual where the public and stakeholders may not have the opportunity to evaluate and comment on any proposed systems.

What the regulations do spend considerable time discussing is the transmission of personal medical information, including direct personal information, between insurers and a third-party vendor known as the Unique Encrypted Identifier Vendor. This vendor serves as an extension of the insurer, collecting sensitive medical information from the insurer, encrypting it, and sending the information back to the insurer for them to connect to their files before uploading files to the APCD. In the absence of detailed criteria, the possession of this sensitive information by the Unique Encrypted Identifier Vendor raises serious concerns about the security of this information during the transmission, and the possession and use of this information once it is in the hands of the Vendor. Moreover, use of the vendor appears unnecessary, as insurers may possess the ability to encrypt the necessary data on their own, using an algorithm provided by the Department; it is our understanding that this is how it is done in the other New England

states possessing similar databases. We believe this was the intent of the General Assembly, as R.I.G.L. §23-17.17-10 clearly states personally identifiable information shall be "protected by the removal of all personal identifiers and the assignment *by the insurer* to each subscriber record of a unique identifier not linked to any personally identifiable information." (emphasis added)

Further expanding on the authority granted under state law, these regulations exempt the information contained within the APCD from the scope of R.I.G.L. §38-2-1 et seq., the Access to Public Records Act (APRA). We know of no statutory authority which enables the Department to make this determination, and as such many of the rules for release of information contained within this regulation may be invalid under APRA. While personally identifiable medical information and other "medical records" are clearly not public under APRA, and therefore cannot be released by any state agency, some of the de-identified information contained within the APCD may be. In this sense, access to certain information contained within the APCD may be subject to release in accordance with APRA.

It is also extremely important to recognize the consequences that flow from collecting a wide range of information potentially identifiable, however indirectly, to individuals, and then establishing a process for releasing "restricted" information. The Department's control over the release of that information may, constitutionally, be more limited than the agency believes. For instance, in an attempt to protect patient privacy, the proposal requires pre-publication review of any proposed public report containing information from restricted release files. Section 7.3(d)(3). However, such a procedure raises basic First Amendment concerns and may not withstand constitutional scrutiny. Further, once the Department acknowledges that these files are available for "improving, evaluating or otherwise measuring health care," the First Amendment may limit

the Department's discretion on who may be entitled to access to this information. See, e.g., *Sorrell v. IMS Health Inc*., 131 S. Ct. 2653 (2011).

Obviously, one of the points of the database is to allow for research that may promote more effective health care. But that goal must be strictly cabined by the need to protect the confidentiality of personal health care information. The process established by these regulations does not, we submit, do that.

In conclusion, we believe there are two main and inter-related themes running through our testimony. First, the regulations should be much more explicit about the security and confidentiality measures that will be in place for the transmission and maintenance of personal data. Secondly, there must be greater limits imposed on the type of personally identifiable information that is submitted and subject to collection and release. It is essential that both of these issues be addressed in order to prevent, as much as possible, the intentional or unintentional breach of very personal medical information, a goal that should be foremost in the Department's mind in implementing this database.

If the suggestions we have made are not adopted, we request that, pursuant to R.I.G.L. §42-35-3(a)(2), you provide us with a statement of the principal reasons for and against adoption of these rules, incorporating therein your reasons for overruling the suggestions urged by us. Thank you for your time and attention to these concerns.