**Legal and Policy Subcommittee of**
**The State of Connecticut Health Information Exchange Advisory Committee**
**Recommendation for Consent Model**

The Legal and Policy Subcommittee of the Health Information Technology Exchange Advisory Committee ("Subcommittee") has carefully considered the various consent models used by health information exchanges ("HIE"). A high level summary of each consent model is attached to this memorandum. We have reviewed the approaches taken by other states in the development of their HIEs and debated the advantages and disadvantages of each of the various models. While some of the states closest geographically to Connecticut have employed an opt-in model, an opt-out model is the consent model used by the most states in the country who have adopted HIEs. An opt-out consent model is generally recognized as the model most likely to result in a successful, viable HIE over time since requiring patients to take affirmative action in the form of consent before protected health information ("PHI") can be collected by the HIE has proven to be a significant impediment in other states.

The Subcommittee has expressed a strong commitment to using the HIE to improve the quality and efficiency of health care provided to patients. Facilitating the exchange of PHI for patient care has been recognized as the highest priority for the HIE. The Subcommittee has also given serious consideration to privacy concerns. Accordingly, the consent model recommended for the HIE follows current federal and Connecticut laws and regulations regarding confidentiality. The only major change to the handling of PHI is the addition of the HIE as a mechanism to move the PHI.

The Subcommittee has deliberately refrained from labeling the consent model it is recommending in order to avoid confusion and to focus on the functions of the HIE as it relates to patient consent. The consent model is based on a presumptive inclusion of all PHI in the HIE with an individual having the right to prohibit disclosure of his/her PHI by the HIE to others. Specifically, the default is for all or some pre-defined set of data (*e.g.*, labs, summary record information) to be eligible automatically for exchange (i.e. collected), with a provision that patients must be given the opportunity to opt out of exchange (i.e. disclosure) of the data. The benefits of this model include, without limitation:

- improving the quality and efficiency of care provided to patients by increasing a health care provider's access health information on a real-time basis and reducing redundancy;
- creating a robust database of health information which can be used on a de-identified basis to develop policy and new programs or to conduct research; and
- facilitating public health activities.

This memorandum is only the beginning of the discussion on development and implementation of the consent model for the HIE. Much additional work must be done to address the detail behind this outline, including but not limited to, addressing certain existing federal and Connecticut laws. The Subcommittee is in the process of performing a Health Insurance Portability and Accountability Act of 1996 ("HIPAA") preemption analysis to identify the Connecticut laws that provide more stringent privacy and/or security requirements than HIPAA with respect to the use and disclosure of PHI.[1] The results of such preemption analysis may result in recommendations for changes in existing or new Connecticut legislation.

[1] The Subcommittee has already identified certain specific Connecticut laws ("Restrictive State Laws") that by their literal terms do not allow health care providers to disclose certain PHI to entities performing a service on the provider's behalf, such as attorneys, auditors, etc. ("Business Associates") without patient authorization.[1] This differs from HIPAA which specifically allows health care providers to disclose PHI to a Business Associate without patient authorization. Despite the literal terms of such Restrictive State Laws, it is customary for health care providers to disclose health information that is protected by the Restrictive State Laws to Business Associates without patient authorization. As such, the Subcommittee will seek confirmation from the Attorney General of the State of Connecticut that a health care provider's disclosure of PHI that is protected by the Restrictive State Laws to the HIE is permitted under Connecticut law.

After much deliberation, the Subcommittee recommends that the State of Connecticut Department of Public Health utilizes the following consent model for the State's HIE.

***Recommendation for CT Approach to Consent Model***

1. Collection of Health Information into HIE
    - Participation in the HIE is optional for providers. Providers cannot submit PHI to the HIE or retrieve PHI from the HIE unless they agree to participate in the HIE.
    - PHI flows from all participating providers for all of the providers' patients into the HIE (no exception).
    - The HIE will enter into a business associate agreement with each participating provider that addresses all HIPAA and federal and state law issues, including but not limited to, inappropriate and appropriate use of the HIE and consequences of misuse. The business associate agreement will meet the requirements of HIPAA but will also serve as a participation or data use agreement, setting forth the terms and conditions for participation in the HIE.
    - The HIE will maintain a Master Patient Index (with a unique identifying number for each patient)("MPI") and a Patient Registry (utilizing the MPI and indexing the locations where data is stored).
        - MPI and Patient Registry maintained on separate servers for security reasons
        - Patient Registry uses MPI to identify locations of PHI

2. Disclosure of Health Information from the HIE
    - HIPAA allows a provider to disclose PHI for treatment, payment and health care operations without patient authorization, except for 1) certain information subject to heightened confidentiality (HIV, alcohol and drug abuse, mental health, etc.) and 2) information subject to a restriction requested by a patient and agreed to by a provider. HIPAA allows a patient to request restrictions on disclosure of such patient's PHI to a person or entity. A provider is not required to agree to the requested restrictions, except in very limited circumstances.
        - The provider who transfers the PHI to the HIE is responsible for identifying PHI that is subject to heightened confidentiality (HIV, alcohol and drug abuse, mental health, etc.)("Sensitive PHI"). Providers have this obligation currently. The HIE will not determine which health information is Sensitive PHI. The HIE will adopt the provider's identification of Sensitive PHI.
        - A provider who agrees to a restriction requested by a patient must convey such restriction to the HIE.
        - HIE will adopt a policy regarding restrictions that will be uniform throughout State.
    - Unless a patient has signed a form requesting that his or her PHI not be disclosed by the HIE, the HIE will disclose PHI other than Sensitive PHI ("Generic PHI"), for treatment, payment and health care operations as permitted by HIPAA, subject to a specific restriction on disclosure agreed to by a provider. Disclosure of Generic PHI will be determined in accordance with existing federal and state laws governing such disclosure.
    - If a patient signs a form requesting that his or her PHI not be disclosed by the HIE, the patient's opt out of HIE disclosures is global. No PHI of a patient who has opted out will be disclosed to any party by the HIE, except as required by law (i.e. public health reporting requirements, etc.).
    - Disclosure of Sensitive PHI (for HIV, alcohol and drug abuse, mental health, etc.) will be determined according to existing federal and state laws governing such disclosure. A

standard form that is compliant with applicable federal and state law will be developed for the HIE.

- Sensitive PHI will be disclosed by the HIE only if a proper authorization is on file at the HIE.

- The different purposes for disclosing PHI from the HIE have been categorized. The priority for disclosure of PHI collected in the HIE is as follows (based on disclosing PHI from the HIE within 1 year, 3 year and 5 year timeframes):
    - Patient Care and Services (need to access data to reduce redundancy and improve care) - Within 1 year
    - Public Health - Within 1 year but recognize could be 3 years due to feasibility issues; Timing of submission of public health data should be split with some data having a higher priority than others.
    - Quality Reporting - Within 3 years
    - Research - 5 years
    - Legal Investigation or inquiry - Future to be determined
    - Other authorized uses

3. Patient Education
    - Each patient will receive a Special Notice from their provider explaining the HIE and the patient's rights regarding disclosure of PHI from the HIE at the patient's first visit following the provider's participation in the HIE. The Special Notice:
        - will be required to be provided by a provider to a patient only one time (like a Notice of Privacy Practices ("NPP") under HIPAA).
        - will be combined with a form for a patient to elect not to have his or her PHI disclosed by the HIE.
        - will include a telephone number and website to obtain more information.
        - will contain an acknowledgement of receipt for the patient to sign to track compliance (like the NPP under HIPAA).

**Core consent options for electronic exchange include the following[*]**

***No consent***

This model provides no opportunity for accommodation of individual preference with respect to participation in electronic exchange, so the health information of patients under the care of a participating provider organization is automatically included in and available (often according to certain rules) through the exchange. This model is typically found in states that require no additional provisions for the electronic exchange of health information beyond the federal floor set by the HIPAA privacy regulations. In these states, electronic exchange can take place irrespective of and without obtaining patient preferences for participation (within the bounds of applicable federal and state laws).

***Opt-out***

In an *opt-out* model, the default is for all or some pre-defined set of data (*e.g.*, labs, summary record information) to be eligible automatically for exchange, with a provision that patients must be given the opportunity to opt out in full. In a typical *opt-out* scenario, this could mean either that the information of the patient who opts out is collected through the exchange (and used only for legally permitted purposes, such as public health reporting), but never shared with other providers for clinical care, or that the patient's preferences are captured and propagated such that his / her clinical information never even enters the exchange. Regardless of where in the system the information exchange is blocked, this option allows for no granularity of patient preference, meaning that a patient's information is either all in or all out. Many electronic exchange models with the legal authority to adopt the *no consent* approach ultimately end up using an *opt-out* approach instead.

***Opt-out with exceptions***

In an *opt-out with exceptions* model, the default is that all or some pre-defined set of data types are eligible for exchange, but patients can either opt out in full (as described above), or: 1) selectively exclude categories of data / specific data elements from the exchange; 2) limit exchange of their information to specific providers / provider organizations; and / or 3) limit exchange of their information for specific purposes. The trade-off with this level of patient accommodation is that it is technically and procedurally more complex to administer and manage. Very few electronic exchange models have allowed for full granularity in the choice of data type exchanged, but some have allowed patient choice as to which provider types may gain access to their data via the exchange. Granularity of exchange at the individual provider level is procedurally more complicated and could pose additional management challenges. For these and other reasons, it has rarely been implemented. Most entities engaging in electronic exchange have not yet attempted to allow granularity with regard to purpose specification, as very few are currently using the information for purposes other than clinical care delivery and public health.

***Opt-in***

In an *opt-in* model, the default is that no patient data are automatically made available for electronic exchange. Patients wishing to make all, or a pre-defined set, of their information available must actively express their desire to participate. This option allows for no granularity of patient preference—meaning that a patient's information is either all in or all out. Once participating, patients who opt in have no control over what information is shared, how, with whom, or for what purpose. The only exceptions here are: 1) permission is later revoked by the patient; or 2) other protections extend to the data (*e.g.*, marketing provisions in the HIPAA privacy regulations).

***Opt-in with restrictions***

In an *opt-in with restrictions* model, the default is that no patient data are automatically made available for electronic exchange. Patients wishing to make all, or a pre-defined set, of their information available

---

[*] This information is taken from the March 23, 2010 *Consumer Consent Options For Electronic Health Information Exchange: Policy Considerations and Analysis* whitepaper, prepared for the Office of the National Coordinator for Health IT: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_911197_0_0_18/ChoiceModelFinal032610.pdf

for exchange must actively grant their consent to participate. They then have the option to make all of their information eligible for exchange or: 1) include only specific categories of data or / data elements; 2) enable information to flow only to specific providers; and / or 3) allow their information to be exchanged only for specific purposes.

In theory, each of these discrete consent models represents a cleanly-delineated option for how patient consent could be approached for electronic exchange. In practice, however, there are as many choice model permutations as entities that participate in electronic exchange. Each entity (regardless of scale) encounters who, what, why, and when decisions, and resolves them based on its own unique set of legal, cultural, political, and other contextual circumstances.