

Testimony to the HIT Policy Committee on
Patient Choice, Control, and Segmentation of Health Information

by J. Marc Overhage, MD, PhD,
 Regenstrief Institute, Inc and Indiana Health Information Exchange
 September 18, 2009

I am pleased to be able to provide the HIT Policy Committee with a case study, based on our real world experience over the last 15 years, of how the we have approached patient engagement in general and individual choice and data segmentation specifically in our health information exchange efforts in Indiana.

The Indiana Network for Patient Care (INPC), developed and operated by the Regenstrief Institute (RI) starting in 1994, provides health information exchange across the State of Indiana. Along with the DOCS4DOCS® clinical messaging platform operated by the Indiana Health Information Exchange (IHIE), the INPC supports health information exchange for over 10 million patients and 12 thousand physicians and their staff. Approximately 50 hospitals participate in the INPC along with independent laboratories, radiology centers, payors, pharmacies and others.

Patient privacy and the security of their health information are and have been fundamental to our health information exchange since its very beginning. We have architected privacy and security into the software, processes and agreements from the ground up with careful balance between them. Our health information exchange subscribes to and implements the principles described in the Markle Foundation’s Connecting for Health Policy Common Framework including “*The Architecture for Privacy in a Networked Health Information Environment*” and “*Model Privacy Policies and Procedures for Health Information Exchange*”, which include:

Privacy and Security Principles

- ✓ Openness and Transparency
- ✓ Purpose Specification and Minimization
- ✓ Collection Limitation
- ✓ Use Limitation
- ✓ Individual Participation and Control
- ✓ Data Integrity and Quality
- ✓ Security Safeguards and Controls
- ✓ Accountability and Oversight
- ✓ Remedies

Adhering to these principles requires both the providers and the health information exchange working in concert. The participating provider must have executed the INPC Participants’ Agreement that ensures they follow specified security and privacy safeguards. These legal, process and policy structures are critical to ensuring the privacy and security of patients’ health information. Providers inform patients, through their notice of HIPAA privacy practices, how the provider will be using the patient’s data. This notification is the primary opportunity for the patient to discuss their wishes around the use and sharing of their data with their provider. The technical architecture underlying the INPC is a centrally managed, federated database model. The provider stores data for which they are the custodian into a database they maintain in a standardized structure using standardized terminology. Patient demographic data from the encounter is used to create a Global (The patient index is global from the perspective of the

providers participating in our health information exchange) Patient Index (a Record Locator Service or RLS in Connecting for Health terminology) that links patient identifiers together across participating providers. The system uses the GPI to create a “virtual patient record” from the participating providers' databases when appropriate conditions are met to enable access for a specific use case. This is a critical concept for the INPC. The conditions that have to be met for a specific use case are established by the INPC Management Committee. These highly specific conditions ensure appropriate limitations on use. For example, in order to create a “virtual patient record” for a provider to use while caring for a patient who has presented to an emergency department for acute care, the following conditions must be met:

- The participant have agreed through their contract with other participants that they follow specified security and privacy safeguards internally
- The INPC has securely received an electronic signal from the emergency department registration system
- The device from which the record is being accessed has to be securely and positively identified as being located at the specific facility (not just the health system) at which the patient has registered for care
- The provider must authenticate themselves to the systems and must have previously been authorized by the institution to access data for use for patient care in the emergency department (the specific use case)
- Access is time limited to 24 hours on the assumption that the specific use case (ED care) would rarely extend beyond that time period.

Other conditions would apply for other use cases such as use of the “virtual patient record” for patient care by a primary care physician in the ambulatory setting, mandatory public health reporting and quality improvement initiatives carried out as part of healthcare operations.

Providers who participate in the INPC decide, with their patients, which data are made available in the provider's health information exchange database. The INPC founders have designed the INPC to recognize the importance of the provider/patient relationship. A patient's understanding and control of his or her data should be topic of discussion between the patient and the provider in which the patient has placed his or her trust to provide health care. Philosophically, those decisions and discussions should not occur between a patient and a technician running a networked health exchange. If a patient and their provider agree that it is in the patient's best interest for certain data not to be shared, the provider does not make the data available in the database. The patient and provider may also decide that the patient wants to be excluded completely from health information exchange. The provider, who maintains the direct relationship with the patient, then notifies the INPC of the patient's request and the INPC staff flags the patient in the GPI so that the system can enforce the patient's desire not to share their health information through the health information exchange.

Ensuring the security and privacy of patients' health information requires carefully attention to all of these principles by both by providers and health information exchanges in a comprehensive privacy protective architecture in a networked environment.