Good afternoon. We appreciate the opportunity to share perspectives on the importance of safeguards regarding the sensitivity and security of patient health information in the IL HIE program.

These perspectives draw upon the collective experience of Alliance of Chicago Community Health Services, a collaboration of Federally Qualified Health Centers which provides Health Information Technology Services to 32 Health Centers located in 11 states, including 10 health centers and safety net practices located in the State of IL. The Alliance has been providing a centrally-hosted Electronic Health Record System to these community based organizations for more than 7 years. Our work has been focused not on the end point of digitizing health records, instead has focused on how to leverage HIT and EMRs to improve the safety and quality of healthcare services.

As community based, primary care practices functioning in a “medical home” model, HIE is seen as essential to improving our ability to support continuity of care, facilitate transitions and more cost effectively manage care across settings such as subspecialty, diagnostic, emergency and hospital services. Our Centers, as well as our patients and communities, see the importance and value of seamless and efficient sharing of information to improve quality and access, and better manage costs.

At the same time, there is appreciation by clinic staff and our consumers that facility of sharing information must be balanced with concern over unintended consequences through sharing of information in ways that can needlessly violate privacy, impair the sense of safety of disclosures within the context of healthcare provider/patient relationship, or lead to negative consequences.

This is especially apparent in Community Health Centers who provide care to vulnerable populations such as Youth/Minors, recent immigrants and refugees, patient impacted by mental health conditions, receiving special services such as domestic violence and substance abuse treatment, and patient’s impacted with HIV & STIs. In each of these cases, it is vital that clients feel safe in sharing sensitive information with their provider who need to work from a comprehensive and complete understanding of the patient’s condition. Because these disclosure currently are often made in the context of a personal relationship, the challenge of HIE is ensuring that both providers and consumers trust that this safety is extended into the HIE through careful attention to how sensitive information is handled.

Strategies to ensure the privacy and safety of this sensitive PHI include the development of a written code of ethics, enforcement of policy and procedures to ensure the safety and security of data, enforcement of existing professional practice guidelines and codes of ethics, and reinforced adherence of appropriate privacy and security regulations. There should be clear consequences and remedies outlined to prevent and mitigate violations. On the other hand it is also crucial that the office of HIT continue to work with the legislature to harmonize the current laws and rules regarding the exchange of this sensitive information, as these uncoordinated standards can lead to unwarranted gaps in critical information needed by caregivers to provide the most optimal and safe care.

In conclusion, the electronic exchange of sensitive patient information presents both challenges and opportunities relative to improve the efficiency, safety, and quality of healthcare services. The IL HIE
program, and the Data Security and Privacy Committee have an opportunity to work collaboratively with healthcare providers, policy makers, consumers and the technology vendors to implement strategies to allow for the exchange of sensitive patient health information while ensuring the privacy and security of this data and the safety of disclosure within the patient/caregiver relationship. This balance can and must be achieved.