Good morning, Chairman Alexander, Ranking Member Murray, and distinguished Members of the Committee. I am pleased to offer you my testimony on a topic that has consumed nearly all of my professional life—the modernization of our healthcare delivery system, and lately, the information blocking that is getting in the way of progress.

I reviewed the previous healthcare IT testimony to this Committee and noted that a very important question has consistently been asked by Committee Members: "How do you define interoperability?"

My definition of interoperability is that every patient deserves to have their complete, longitudinal medical record available wherever and whenever decisions are made about their health. "Wherever" includes places like the doctor's office or the emergency room, between doctor visits when medications are refilled, as well as at home with the patient or caregiver and on smartphone when the patient travels.

I think this definition is helpful because it reminds us that the primary objective of interoperability is to better serve the patient. It also provides us with a convenient test for any health IT implementation or policy. "Does my EHR ensure that my patients have their records from my clinic available no matter where they seek care?" is a fundamental question all doctors should ask about their systems.

Another important test is ensuring that each patient, and population, is receiving high value care—the primary ingredient required for successful value-based payment models. In order to do this, quality and cost measures must contemplate ALL of the relevant data on each patient. Since the average patient sees more than 3 different doctors each year, and the average Medicare patient sees 7, this almost always means aggregating data from multiple doctors and hospitals in order to get an accurate picture of individual and population health. To do otherwise would be like assessing the record of a football team based only on the performance of the left tackle.

We in Oklahoma have been hard at work transforming our healthcare delivery system. MyHealth Access Network is a non-profit health information exchange organization serving more than 4 million patients and connecting 275 organizations, including doctors, hospitals, pharmacies, tribal health systems, payers, employers, home health, hospice, long term care, state and local agencies, and many others. MyHealth received a Beacon Community Award from ONC in 2010 which encouraged and enabled us to build the Oklahoma approach to interoperability.

MyHealth has established effective health information exchange with dozens of EHR's, administrative systems, and payer claims systems, and consolidates this data into a single record for each patient to ensure that their complete medical record is available wherever, and whenever needed for care. In addition, MyHealth serves as the entity most trusted by payers and providers to measure quality, cost, and value in support of new healthcare payment and delivery models. This unique Trusted Third Party arrangement has accelerated the adoption of value-based payment models in Oklahoma, and has enabled providers to succeed in these new care delivery models.

For example, under the Beacon program, MyHealth demonstrated significant improvements in critical ACO success measures: preventable admissions and ER visits for asthma, COPD, and congestive heart failure. MyHealth technology has been shown to improve care transitions by reducing wait times for access to specialty care by 2/3 and significantly reducing the total cost of care for transitioned patients in the Medicaid population.

MyHealth has also served as the Convening organization and data aggregator for the Oklahoma implementation of a CMMI pilot project called the Comprehensive Primary Care initiative (CPC), which includes local commercial payers as well as Medicare and Medicaid in Oklahoma. These multiple payers have partnered to implement a value-based payment and practice transformation program in primary care practices. In the first year of the program, Oklahoma's 65 CPC practices reduced Medicare costs by 7%, prompting Secretary Burwell to seek commentary on the potential expansion and permanent implementation of the CPC model in the latest CMS Physician Fee Schedule.

These accomplishments have been hard fought, requiring more than 5 years and $15M to produce. By far, the most significant barrier to success has been liberating accurate patient data from practices, hospitals and other organizations.

Generally, we think of data blocking as the intentional interruption or prevention of interoperability by one of two parties: the Provider or the Provider's EHR vendor.

Provider data blocking may have been an important challenge early in the development of MyHealth but it has quickly receded as value-based payment models take hold. The Comprehensive Primary Care initiative, the rise of several ACO's, and important moves by commercial payers such as Blue Cross and Blue Shield have all combined to convince providers in Oklahoma that value-based payment models are the present and the future. CMS further endorsed this thinking with their announcement in January. As providers recognize that their success in these new models of care and payment is dependent on having their patients' comprehensive data available wherever it is needed for decision-making (even if that is a competing organization), the provider-driven barriers to interoperability tend to melt away.

Thus, the biggest challenge we face is helping our willing provider members to liberate the patient data from their EHR systems to make it interoperable. We have so many specific experiences with inappropriate data blocking and substandard data quality that we have created a nomenclature to classify the 6 common types. We have had some success in solving these issues, but many remain unresolved. Below we describe each type of data blocking in the context of a real event.

Before reviewing the examples, I would like to point out three things. First, many EHR vendors work well with their customers and with our organization to establish interoperability. Second, until recently, we have been left with few options to address most data blocking issues. We have become active users of the ONC Certified EHR Technology Surveillance program, filing complaints after we have exhausted all other efforts to work with the vendor and the provider to implement interoperability. Finally, the cases below are examples of the types of issues we have experienced, but these issues arise in most other communities as well.

Type 1: The Golden Rule

By far the most common barrier to interoperability, exorbitant interface and maintenance costs cause many small practices and hospitals (and some large ones) to forego participation in HIE or at least providing data to the HIE. The EHR Certification requirements do not set parameters for the fees that vendors may charge for interoperability, so this is a very common barrier.

In our experience, typical, acceptable interface costs are below $2,500 per practice. However, several well-known vendors charge $10,000 or more per practice, regardless of practice size, and some charge

more than $30,000 to $40,000, which for many practices in Oklahoma amounts to $3-$5 per patient seen for an entire year.

Other vendors charge per patient. One vendor in particular has, until recently, charged more than $2.00 per patient per year, which added nearly $1M in cost to large health systems and prompted an avoidance of the standard interface approaches with that vendor. Asking a CFO to pay $1M extra just to provide competitors with access to see their patient data seems silly, but is exactly what this per-patient per-year fee model does.

When we question vendors about the exorbitant cost of interfaces, we are often told they are technologically complex and labor intensive. While this may be true, the complexity is usually a result of the vendor's own decisions about architecture and their implementation of the meaningful use interoperability requirements. In addition, it is difficult to recommend to our participating providers that they pay these fees when a number of well-known EHR vendors have been extracting the data from their customer's practices, de-identifying it, and selling it for years. Certainly this process is more technologically complex than making a standards-based interface for clinical data.

Type 2: The "Hotel California"

There is a component of the EHR Certification program called "data portability" that is intended to help providers to change EHR vendors if they like. Vendors are required to enable providers to create a batch export of their patient records in a standardized format. It is also a very helpful capability for interoperability. Unfortunately, few vendors appear to offer this functionality as intended, and so we say that the customers of these Vendors have a Hotel California problem-- they can check out other EHR products any time they like, but their data can never leave.

MyHealth has filed complaints about this issue our initial complaints have been found to have merit by ONC and the ACB, but no specific timelines have been provided. Thus, doctors using this Vendor's EHR are facing pressure to meet Meaningful Use by the end of the year without a clear idea of whether, or when, the product will enable them to do so.

Type 3: The inexplicable.

In some cases, the reasons for data blocking are not clear, and do not seem to be linked to any specific technology limitation or business driver. Often, given time, the real motivation behind the data blocking will become clear and it usually resolves to a vendor- or provider-driven decision about cost.

For example, during the install of a major comprehensive EHR product in one of our largest health systems, we were told by the Vendor's project manager that "We don't *do* CCD's, they're just not in our DNA". We pointed out that their product was Meaningful Use certified, implying their ability to produce a CCD (a Patient Summary of Care file), and, in any case, this was their customer's request. Despite an hour of questioning, the project manager remained unfazed and simply continued to repeat "we don't do CCD's, they're not in our DNA".

This issue remains today, despite the fact that we now get CCD's from other instances of this vendor's product. We were forced to build and maintain 5 different HL-7 (an older protocol, still heavily relied upon in healthcare) feeds to replace the missing CCD. The missing data from this health system means

that their patients are at higher risk of Adverse Drug Events, duplicated testing and imaging (and radiation exposure).

Type 4: Garbage in, garbage out.

All certified EHR's are required to produce Patient Care Summary records according to a common format, but many of them fail to include the proper structure, clinical content, or standard codes. We have never seen a completely correct Patient Care Summary despite processing millions of them.

Poor data standardization and quality prevents data from being combined with other records on the patient, creating a messy and often inaccurate chart riddled with duplications. Further, this prevents the calculation of metrics and care gaps, as well as quality measures, compromising the safety and accuracy of clinical decision support, and undermining the success of value-based payment models.

Type 5: EHR at the center of the universe

Increasingly, we are hearing from large health systems using certain EHR systems that their EHR vendor provides all of the interoperable information they need. These vendors have done an excellent job of implementing interoperability with other health systems using their EHR products. However, this interoperability does not extend beyond the specific vendor's customers, excluding independent providers and small hospitals, pharmacists, ancillary care services and long term care, etc.—all of which play a critical role in the health of patients.

Most concerning about this belief is that it subverts interoperability at the community and state level, creating instead a corporate EHR network for interoperability, which is not subject to the trust arrangements and policies of the community.

Type 6: The "bait and hidden switch"

In this type of data blocking the vendor achieves certification with one feature set and then either hides or eliminates functionality when the EHR is deployed in a practice or hospital.

We pursued interoperability for nearly 4 years with one of the nation's largest ambulatory EHR vendors, but were told repeatedly that we must purchase their proprietary "HUB" product. In addition to a base cost of $40,000, the HUB carries an additional monthly service fee of $50-$100 for every provider in every practice—more than doubling the cost of HIE services.

Recognizing that 2014 EHR Certification required them to produce the Patient Care Summary files for interoperability, we filed a complaint with ONC, which was forwarded to the Accredited Certifying Body (ACB) for the Vendor, who apparently forwarded the message to the Vendor.

Almost immediately we received an email from the Vendor indicating that they would no longer work directly with our HIE. We were quite surprised and concerned, but fortunately, within a few hours, we received an email from an executive with the Vendor. Realizing that the certification challenge was credible, the executive offered some new information, unknown to any other practice or HIE in the country, as far as we can tell. It turns out that instead of requiring the purchase and implementation of the HUB product, the vendor could make a simple "configuration" change to enable the data to flow out of the system. We immediately requested that the configuration change be made in our participating

practices, and by 10AM the next day we had data flowing from three practices, at no additional cost to the providers.

The EHR Vendor product had passed certification testing with the configuration switch turned on, but turns it off by default for every installation of the product. Until we filed this challenge, no amount of direct questioning of the Vendor support, sales, and implementation staff revealed the existence of this "switch".

The follow-on story is also informative. This feels to us like an important product defect that would be communicated to customers in any other industry. Since most of these installations were funded with tax-payer dollars, it would seem that the commitment to transparency would be even greater. Unfortunately, the Vendor does not appear to be communicating this information to their customers, and continues to offer the expensive HUB as the only way to get data out of their EHR system. So, we have shouldered the burden of informing the public and relevant stakeholders, including our HIE colleagues. We have assisted several states in making this configuration switch work for them, and we are happy to do it—but we continue to ask why a formal and transparent communication process is not being required.

Of particular concern to me has been the clear reluctance on the part of the practices to file or participate in the filing of complaints against their EHR vendors. Several times, affected practices have requested MyHealth to file the formal complaints on their behalf, but expressed fear that filing directly could prompt retribution from the EHR vendor. I have been surprised to find intimidation of providers by their vendors, whether real or perceived, playing such a significant role in the data blocking issue.

Recommendations:

I have several suggestions to address and prevent the issue of data blocking.

1. The HIT Certification program is the strongest lever available to ensure Vendor alignment with success of the nation in achieving the optimization of health and quality of life for all Americans. I recommend a tuning of the initial certification and an expansion of the ongoing surveillance program.
    a. Initial and ongoing certification recommendations:
        i. Current testing: EHR's are currently certified based on testing in an ideal, laboratory environment.
        ii. Expanded Certification Testing: We recommend that certified EHR's have their interoperability functions tested in the field with each deployment of their product in order to maintain certification. In this way, the product can be proven to be interoperable before the "keys" are handed over to the provider. This would specifically address Information Blocking Types 2, 3, 4, and 5 above. We are happy to expand on ways this can be accomplished cost-effectively as requested.
        iii. Meaningful Use 3 Proposed requirements: It has been proposed that Certified EHR's must enable providers to choose standard clinical documents and schedule them for automated delivery to specific locations based. Preservation of this requirement is critical to achieving broad interoperability.

b. Certification Surveillance program recommendations: As noted above, most progress on addressing the data blocking issue has come through successful use of ONC's Certified Health IT Surveillance program. We propose expansion and amendment of this program in the following ways:
    i. More prominent role: The ONC Surveillance program can be very important in solving these issues, but it must become a more prominent component of the Certification program to have maximal impact. Doctors and hospitals need to know how and when to use it, and Vendors need to know what to expect from it as well.
    ii. Increased Transparency:
        1. When a complaint is found to have merit, and changes have been requested of a specific vendor, the customers deserve to know the details and timing for a solution. Posting the adjudicated issues and timelines will enable providers to plan and increase trust among the provider community.
        2. An annual Health IT Surveillance report has been produced by the Accredited Certifying Bodies, but the report is only accessible via a Freedom of Information Act request—creating an additional barrier to transparency and therefore trust.
    iii. Whistle-blower protections: As described above, many providers, especially small clinics and hospitals, are concerned about backlash from their vendors that filing a complaint may generate. Whether these fears are warranted or not, it's important to create an environment where these providers can feel safe in airing their concerns.
    iv. Independence from Conflict of Interest: Currently, the Accredited Certification Bodies, who are responsible for the Certification program, are also responsible for executing the Surveillance program. This could be perceived to be subject to conflict of interest, since the ACB generates nearly all its revenue from the Vendors that it certifies. For example, an ACB perceived to be overly strict by Vendors could lose its Certification business.
c. Lemon law for EHRs: On more than one occasion in our community, providers have invested heavily in an EHR product, only to discover that it does not meet their needs. One small, financially strapped hospital in Oklahoma recently fired their EHR vendor when it became clear that the Vendor would not meet 2014 EHR Certification—which would prevent the hospital from meeting its Meaningful Use obligation. Unfortunately, the EHR vendor sued the hospital for breach of contract.
   An appropriately crafted Lemon Law could help to prevent these kinds of issues.
d. Transparency in contracting: The contents of EHR vendor contracts are among the best kept secrets in America, and the signatories are often bound by strict non-disclosure agreements. Certain elements of these contracts, and specifically those pertaining to interoperability, should be made transparent to customers and other healthcare stakeholders.

2. Payment model incentive alignments provide the strongest incentive for providers and hospitals to support and enable interoperability. In particular, the expansion of value-based payment

models are prompting providers to look beyond the walls of their organization for the patient information they need.

   a. In the short term, a process measure for interoperability should be employed to help providers and other stakeholders gauge their progress in achieving appropriate levels of interoperability. We have defined several measures that could be of use and would be happy to share them.
   b. CMS and other federal partners such as the DoD, VA, and HRSA should begin to place more value on Clinical Quality measures derived from a comprehensive record of the care each patient receives, rather than from a single EHR or site of care. This will further encourage provider participation in meaningful health information exchange, and will significantly improve the accuracy of the quality measures being reported. In Oklahoma, the commercial payers and Medicaid have already recognized the importance of this approach to value measurement and are proceeding to implement it.
   c. Support the development of regional data aggregation such as HIE's and the implementation of whole-patient quality reporting. These are important infrastructure elements that are needed to support the kinds of measurement described above for value-based payment programs, and also to ensure that patients get comprehensive, safe care no matter where they seek it.

3. Standards: It may be controversial for me to say this as a Board Certified Medical Informaticist, but we have plenty of standards—we need to focus on correctly implementing the standards we have right now and monitoring their performance. R&D on new standards should continue, but they should undergo rigorous testing before becoming a part of the certification or meaningful use requirements. The ONC Standards Advisory hits the mark well on this issue.
4. Governance: This is perhaps the most critical issue limiting the impact of the tax-payers $30B investment in health IT. In the original HITECH act, ONC was called upon to establish the governance for the nationwide health information network. Now, more than six years later, that governance still does not exist, due in part to interpretations of limitations on ONC's authority. Thus, there is a vacuum in governance for this critical component of America's infrastructure—and that vacuum is being filled by various consortia and collaborations of vendors and large provider organizations. In order to rapidly advance health IT and interoperability, ONC's authority should be made clear, and I believe strongly that the correct perspectives to include in that governance are:
   a. Those who receive care (patients, special population representatives)
   b. Those who deliver care (providers, public health), and
   c. Those who pay for care (payers, employers, governments).

Thank you for this opportunity to share my experiences and offer my advice. The progress made to date is tremendous, and I am confident that with your guidance, health and healthcare in America can become the best in the world.