

Good afternoon Chairmen Stark, Ranking Member Herger, and other distinguished Members of the Subcommittee. My name is Jonathan Hare, and I am the Chairman and Founder of Resilient Network Systems, which is a software company headquartered in San Francisco. I thank you for the opportunity to appear before you today.

To begin, I would point out that virtually everyone in this room no doubt agrees that widespread adoption and use of health information technology is essential to transforming America's healthcare system, and that the HITECH Act represents a unique opportunity to accelerate that adoption.

Eighteen months have passed since the law was signed, and now that the final rule for Meaningful Use reimbursement has been published, it is worth asking what progress has been made, and what the prospects are for actually achieving the benefits HITECH is intended to deliver.

My answer is that while much has been accomplished on many fronts, there has been almost no visible progress in addressing one crucial challenge that is essential to achieving the aims of HITECH. Specifically, I refer to the need to establish a nationwide capability for secure exchange of health information among patients and their caregivers while protecting patient privacy.

One of the things I like most about the HITECH Act was that it recognizes that the deployment of information technology by itself isn't sufficient. What matters is how it is used, and who has access to the information and decision support that it enables. Indeed, the vast majority of the benefits from health IT depend upon the ability to connect and share data among patient and their personal network of caregivers, to provide timely decision support, and to help patients be proactive in their own care.

It is for this reason that the HITECH Act specifically provides that in order to qualify for the meaningful use incentive payments, eligible professionals are required not only to use certified EHR technology in a meaningful manner, but also to demonstrate that

such EHR technology is *connected* in a way that provides for the electronic exchange of health information. This language can be found in on pages 355 and 356 of the Act, in Subtitle A, Section 4101.

The recently released Meaningful Use final rule acknowledges this requirement by including as a core objective “implement the capability to electronically exchange key clinical information among providers and patient-authorized entities.”

Unfortunately, the measure specified in the final rule for 2011 and 2012 is to “perform at least one test of the EHR’s capacity to electronically exchange information.” There is no requirement to implement authentication, consent, authorization, disclosure management or any other services specifically mentioned in the HITECH Act that are necessary to genuinely enable secure electronic exchange of information. Moreover, the test can be performed with “dummy” data for a “fictional patient” in order to avoid “privacy and security concerns”.

My view is that this measure is not really exchange, and comes nowhere close to what was intended by Congress when it passed HITECH. It also stands in stark contrast to the other core objectives in the rule, each of which require that they be met for a significant percentage of patients, most of them 50% to 80%.

The comments in the notice of the final rule justify the virtually non-existent requirement for HIE by stating that “many areas of the country currently lack the infrastructure to support the electronic exchange of information”. I disagree with this rationale and think it is a serious mistake, for three reasons.

First, based on numerous discussions last summer with Congressional staffers involved in drafting the HITECH Act, the meaningful use incentives really were intended to be incentives, not entitlements.

The staffers I spoke with were painfully aware of the repeated failures of previous attempts at health information exchange, and the fact that traditional EHRs “weren’t built to share”. I was told that the HITECH Act’s \$30 billion in meaningful use payments was intended to create an incentive not just for providers, but also for the vendor community and technologists to figure out a way to overcome historic obstacles to HIE. The reason the initial payments were deferred for two years until 2011 was to give

time to innovate and prepare – not to give time for lobbying to water the requirements down to something existing solutions could accommodate.

Second, by eliminating any real requirement to enable health information exchange until 2013, the final meaningful use rule dramatically undermines the incentives to innovate and invest in enabling real HIE.

Necessity is the mother of invention. By eliminating the necessity for HIE in order to receive incentive payments, the final rule eliminates the incentive to invent or develop the capabilities necessary to achieve it. This creates a vicious cycle where the lack of incentives breeds lack of investment and innovation, translating into a continuing lack of HIE capabilities, in turn justifying further deferral of requirements for real HIE in order to receive incentive payments.

I have seen evidence of this already in the plans from state HIE organizations, many of whom have interpreted the 2011-2012 meaningful use criteria as de facto permission to defer serious efforts to address the core network services necessary to enabling real HIE. Phrases like “back-burner” and “out-of-scope” have become common place when discussing the enabling infrastructure for HIE.

Third, I strongly disagree with the presumption that secure health information exchange is not feasible in the 2011-2012 timeframe. The infrastructure necessary to enable data interoperability exists, has been successfully demonstrated many times, and is deployed today. The problem has been a failure to develop a viable approach to connecting applications into a trusted network that enforces security and privacy, and gives patients sufficient control over their own data.

The traditional models for sharing health information while protecting security and privacy have repeatedly proven woefully inadequate in practice, and are incapable of satisfying the requirements of the HITECH Act. I would describe this approach as somewhere between a polite fiction and a fantasy. It is a great way to spend money on HIE consultants and vendors, but repeated experience has shown it just won't work.

I believe a different approach is possible, a patient-centric network capable of enforcing robust security and privacy policies on a national scale. Such a network would have able to conveniently authenticate and verify identities of any patient,

provider or caregiver; provide robust security enforcement regardless of where data flows; enable consent and authorization management, records retention and disclosure management; allow organizations to provide access to data without losing control of it; and allow patients to access their own data, keep track of who is accessing it; and selectively restrict access if they choose.

With proper support such a network could be fully deployed, tested, certified and rolled out on a national scale within a year, making it possible for providers to really earn their meaningful use incentives, thereby laying the foundation for realizing the potential of the HITECH Act.