WRITTEN TESTIMONY OF DR. BRUCE TAFFEL
CHIEF MEDICAL OFFICER, SHARED HEALTH®
NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS
SUBCOMMITTEE ON PRIVACY, CONFIDENTIALITY AND SECURITY
DEPARTMENT OF HEALTH AND HUMAN SERVICES
MAY 21, 2009

Chairman Houston, Chairwoman Francis, Members of the Subcommittee, fellow panelists: I appreciate the invitation to join you for a discussion on a topic that stands at the intersection of our nation's goals on health care—improving care, reducing costs and, of course, the vital mission of this Subcommittee: protecting privacy.

My name is Bruce Taffel, and I am the Chief Medical Officer of Shared Health®, one of the nation's largest public/private Health Information Exchanges. I am here first and foremost as a physician who knows that the quality of medical care depends on the quality of medical information. More and better medical information exists today than ever before. But this information is stored in silos—from physician offices to pharmacies to insurers—preventing providers from considering the totality of a patient's clinical conditions and needs.

Within that problem lies this possibility: These silos store enough information to paint a complete, detailed and accurate picture of a patient's health—if that information can be integrated and made easily available to both patients and providers. That is the purpose—the mission—of Shared Health: To improve outcomes, safety and efficiency by providing authorized healthcare professionals at the point of care with patient-centric communities of health care information, clinical decision support services and population health management tools.

We envision a day when each patient can make fully informed decisions and receive the best care because every provider with whom he or she comes into contact, from specialists to pharmacists, has a complete portrait of his or her health—a portrait that evolves with time and follows the patient throughout treatment. The result will be better care, delivered more efficiently, at a lower cost.

For many, the goal we envision remains exactly that: a vision. However, for more than 2.6 million patients who participate in the Shared Health® Clinical Xchange™, as well as more than 3,800 clinicians who care for them, it is a reality today.

In these remarks, I hope to explain how Shared Health is realizing this vision while protecting patient privacy, as well as the opportunities and obstacles we see ahead.

How Shared Health Works

Shared Health works to improve clinical outcomes by providing a single view of patient data to both clinicians and patients. We are a steward of information: Rather than owning patient data, Shared Health holds it in trust. We offer a patient-centered information exchange with tools that enable our stakeholders to manage care better. To build this exchange, Shared Health collects and integrates medical information on participants from multiple sources, including payers, clinicians, inpatient and outpatient facilities, laboratories, pharmacies and pharmacy benefit managers. We offer a hybrid data model that combines a federated approach supported by a repository that merges a limited data set of key clinical indicators with administrative data. This repository makes data available for Clinical Decision Support processing. The comprehensive picture of a patient's health developed from this data is available online in the Shared Health Clinical Health Record® (CHR) for clinicians whom we have authenticated and educated on our privacy practices.

Shared Health's revenue comes from a variety of sources, including payers, employers, government and providers. Our business model begins with payers—such as insurers or state Medicaid programs—who invest in Shared Health in order to improve care and lower costs. Employers who provide benefits through commercial payers allow Shared Health to steward the medical information of their employees, who, in turn, have the right to opt out of the system if they choose. Very few employees—fewer than one-tenth of one percent—do so because we carefully and comprehensively explain both the potential benefits to their health and also the stringent safeguards implemented to protect the security and privacy of their information.

We provide new participants with several informational documents that include an introductory welcome letter; a new member packet; notification that participants' health care providers have access to their electronic health record; a letter explaining the opt-out option as well as an opt-out form; and, finally, a request form for each participant's health record. We have found educational efforts addressing privacy, security and potential health benefits to be both vital to and successful at encouraging participation. And we are and must always be clear: Information collected for clinical use should not be shared with employers or insurance companies for the purpose of underwriting except with consent.

In order to protect the clinical integrity of the data we collect, it can only be amended by authorized users—although, as HIPAA requires, patients are allowed to review and request amendments to information that is identified in a designated record set. When these amendments are not made, the information is annotated to indicate that it has been disputed.

An important part of Shared Health's value is adopting standards and semantic taxonomies supporting interoperability. We have the ability to accept literally any data related to a clinical event or transaction and collate it alongside events from other healthcare trading partners, regardless of the format or terminology used. Shared Health

emphasizes a Services-Oriented Architecture (SOA) through which best-of-breed components communicate through web services and messaging with minimal need for customization. We use national and even international standards to gather, normalize, store and share health information. And this system is highly scalable.

Using this system, any authorized provider can instantly access accurate and comprehensive data on the patients in their care. Patients and families do not have to memorize and repeat technical medical information, nor must they clean out their medicine cabinets and bring a brown paper bag full of medications to a doctor's visit. This system has the potential of sparing sons and daughters the agonizing burden of reconstructing medical histories for their ailing, elderly parents. There are no delays while charts are copied, faxed or mailed. Clinicians use online tools to write electronic prescriptions that are instantly transmitted to pharmacies and recorded for other providers to see. Adverse drug events resulting from poor handwriting, limited information and drug-to-drug interactions are reduced. Formulary compliance and better utilization of cost-saving generics are reinforced.

And the payoff in better care and lower costs is clear. Clinicians are more informed about each patient's health history, clinical needs and treatment recommendations. Using Shared Health, clinicians in Tennessee have lowered readmissions by 29.8 percent, reduced services needed in the emergency room by 40 percent and brought the average length of a hospital stay down by 20 percent. Treatment efficiency is up by 17 percent, and other costs are falling too—a 21 percent reduction in emergency room visit costs and an average of $8 less per prescription.

Shared Health is proud of this success, and we urge you to hold us, other CHRs as well as PHRs accountable for continued improvement on the measures that matter: the health of the people on our platforms and the cost and efficiency of care.

The success we have already documented in improving the quality of care, achieving better health outcomes, enhancing efficiency and driving down the total cost of care is only the beginning. We have seen a large amount of interest in and usage of our platform by clinicians and hospitals and expect it to continue to grow, especially in the hospital arena. Utilization of Shared Health solutions is already climbing at a rapid pace. Between February 2008 and March 2009 alone, monthly patient lookups by providers rose more than fourfold, from 10,000 to more than 40,000. Over the same period, the number of electronic prescriptions grew from approximately 2,000 per month to more than 25,000 per month. We believe healthcare reform that emphasizes reimbursement based on quality and outcomes will further bolster usage of our tools and services.

Security and Transparency

Of course, none of this success could or should be possible without our strong focus on patient privacy. Our security system is the bond that links Shared Health with consumers by enabling them to trust us with their information. Consequently, Shared Health maintains a culture of transparency with regard to privacy and security practices. We

offer information on our website that addresses privacy and security concerns. We are available to attend face-to-face meetings with employers and health plans that are upcoming participants in our HIE. Shared Health also has dedicated email addresses at which consumers can reach privacy specialists who can answer specific questions. Our customer support lines have access to resources that deal with individuals' privacy or security concerns as well.

Shared Health's commitment to privacy is also evident in our systems. Our privacy safeguards exceed the minimum requirements under HIPAA. Shared Health provides all individuals with their rights as prescribed under HIPAA, such as an accounting of disclosures outside of TPO, access to their information and the ability to request an amendment to their information. We absolutely believe any records that contain a member's medical history—including PHRs—should be subject to current and future HIPAA privacy and security rules.

In addition to those minimum protections, Shared Health provides an audit trail report to each individual who requests it telling them what organization accessed their record and when. Our procedures for auditing of system logs include but are not limited to failed attempts to access files, resources and other objects; successful attempts to access information; logon successes and failures; account creation and maintenance; dial-up activity; firewall activity; and other security administration activities. All information and critical details are logged.

Shared Health incorporates processes in data collection to ensure that sensitive information is protected from unauthorized disclosure. Currently sensitive information is filtered from the data input process to ensure compliance with multiple state and federal laws and regulations. Certain types of records are routinely not included in Shared Health's Clinical Health Records, including sensitive and protected information such as sexually transmitted diseases and chemical dependencies.

While as an HIE, Shared Health accepts data from our contributors, we also have processes to ensure data subject to the HHS Substance Abuse rules, if received, is appropriately protected. However, it is not a simple task. There are many locations where these diagnostic codes may be stored, and we are very diligent in identifying and masking those locations.

We also impose a strict screening system to ensure private patient information is accessed only by authorized users. The Shared Health solution requires that all users initially register with our HIE in order to authenticate their identities. In addition to registering with us, participating clinicians must also be registered with the National Plan and Provider Enumeration System and provide their National Provider Identifiers, the unique codes assigned to providers and health plans under HIPAA. Our system will respond only to queries initiated by authenticated, authorized users.

Future Issues and Opportunities

As you know, a number of potential regulatory and other issues lay ahead. For the benefits of HIT to be fully realized, networks must be as seamless as possible. Consequently, Shared Health favors replacing the patchwork of state regulations with federal standards that would make administration and privacy rules more consistent. The optimal position for sensitive data would be a federal standard that would preempt all state disclosure requirements for the sharing of information for treatment purposes. There should be a single set of policies for accessing protected data so that a standard break-the-glass feature would adequately protect information but allow access to important data in exigent circumstances such as emergency care.

Shared Health believes privacy issues should be viewed through the lens of providing timely and effective patient care—and, furthermore, that those goals are completely compatible. Security systems can and must adequately protect patient privacy without causing either needless delays that impede adoption of the technology or potentially dangerous delays in emergency situations.

For that reason, we are concerned about one aspect of the implementation of the Recovery Act. In its current form, the proposed guidance on the definition of technologies and methodologies that render PHI unusable, unreadable, or indecipherable could create a substantial impact on system performance and provision of information in real time at the point of care. Encryption of data at rest has been a longstanding debate among privacy and security advocates. In our experience, if it takes more than 30 seconds for an authorized user to retrieve patient data from the HIE, it hinders integration of the technology into physician workflow and reduces overall adoption of the tools.

Shared Health will continue to monitor the guidance published by HHS on the modifications to HIPAA over the coming months. As a covered entity, Shared Health already complies with the original version of the HIPAA privacy rule. Shared Health will continue to review our policies and procedures as a result of the changes in ARRA, but because our privacy policies and procedures already exceed HIPAA requirements, the impact to our operations will not be as substantial as to some PHR vendors.

We have learned that education is the key to ensuring consumers understand privacy issues accurately and to building the consumer trust on which adoption of HIT depends. It is essential for the public to understand the importance of systems that protect privacy while allowing providers quick access to the information they need to provide better care. The public is not yet fully engaged in this conversation, so it is unclear how informed consumers are as to their needs, as well as how much they know about where information is used; when it is important to have access to it; and what constitutes improper use. There are misconceptions we must address as well. For example, some consumers inaccurately believe that web-based systems are available for anyone who can access the Internet. An educational effort must address all these issues in order to realize the full promise of HIT.

Moreover, in developing privacy policies, we have grappled with a number of questions that bear continued discussion. What constitutes sensitive information? What are the implications of medical ethics with regard to "need to know"? This question can become pertinent in emergency room situations or in scenarios in which one patient's rights may affect another's, such as a potential conflict between the health of a newly born child and the privacy rights of a mother with chemical dependencies.

In addition, as noted in NCVHS' February 20, 2008, letter regarding individual control of sensitive health information, should sensitive data be available for Clinical Decision Support system processing? The medical community has also raised questions about liability concerns if providers rely on a record that is incomplete or does not identify gaps in information availability. And, as I indicated earlier, how do we keep the provider engaged with rapid performance; access to timely, relevant data; and ease of use while also protecting privacy?

Finally, allow me to conclude by saying that the full promise of HIT is immense. Even the remarkable possibilities we have already seen are only the foundation for the innovation still to come. In the coming years, patient-facing online services will increase access to health care choices and transform today's consumers into collaborative participants in their own care. Engaged consumers will work with all the constituents of their healthcare teams to direct a seamless flow of data that will follow them and guide all the clinicians participating in their care. Evolving technologies will increasingly inform and empower patients, giving them enhanced control of their personal information and treatment. Growing interoperability will relieve patients and their families of the overbearing burden of being the sole messengers of complex medical information. And the results will be remarkable progress toward the goal our country shares: better patient care, delivered more efficiently, at a lower cost. Thank you.