



Office of the National Coordinator Health Information Technology
Department of Health and Human Services
Attention: NHIN RFI Responses
Hubert H. Humphrey Building, Room 517D
200 Independence Avenue, S.W.
Washington, DC 20201

BY ELECTRONIC MAIL

**Response to Request for Information on “Development
and Adoption of a National Health Information
Network”**

January 14, 2005

CONTACT:

The Liberty Alliance

Telephone: +1 (732) 465-6475 (8:30am-5:00pm EST)

FAX: +1 (443) 647-0099

Email: info@projectliberty.org

Table of contents

1. Introduction.....	3
2. Responses to Questions	5
General.....	5
Question 1	5
Question 2	6
Question 3	6
Organizational and Business Framework.....	7
Question 4	7
Question 7	7
Question 8	8
Management and Operational Considerations	8
Question 10	8
Clinical scenario/Use case for Liberty specification in NHIN encounter.....	10
Standards and Policies to Achieve Interoperability	13
Question 14	13

1. Introduction

This document constitutes the response of the Liberty Alliance Project (hereinafter “Liberty” or “LAP”) to the above-captioned Request for Information, as published in the Federal Register on 15 November 2004 (69 Fed. Reg. 65599).

Liberty is offering this direct response and also participating in the joint filing authored by the Markle Foundation, HIMSS, the AMIA, ANSI and a number of other organizations (“Joint Filing”). We are taking this approach in order to profile and provide emphasis in a number of areas in which we believe Liberty and its members possess useful unique expertise, the detail of which is beyond the scope of the Joint Filing.

We do this in the hope that these additional remarks will amplify the points in the Joint Filing, in particular on matters related to NHIN technical architecture and the technological means of achieving system interoperability across the diverse set of institutions envisioned as participants in a fully functioning NHIN.

The Liberty Alliance Project is an unincorporated association of more than 150 organizations, including leading banks, technology companies, government agencies, wireless providers and other companies and entities from around the globe. Liberty is committed to developing an open standard for federated identity that can operate across diverse platforms and devices. Federated identity offers businesses, government, employees and consumers a more convenient and secure way to control identity information in today’s digital economy.¹

The Liberty Management Board, which determines direction for the Alliance, is made up of 16 members, including: America Online, American Express, Ericsson, Fidelity, France Telecom, General Motors, Hewlett-Packard Company, IBM, Intel, Nokia, Novell, Oracle Corporation, RSA Security, Sun Microsystems, VeriSign and Vodafone.

We firmly believe the adoption of federated identity is key to making a national health network viable. Liberty sees this as a national network connecting sub-networks, users and other participants instantaneously while protecting the privacy and security of all involved.

As prologue, Liberty wishes to address several contextual issues which may clarify our intent in filing this document.

First, while Liberty represents a community of more than 150 organizations across diverse sectors, its roots are among the vendor institutions which have developed and enabled the network environment we presently refer to as the Internet or Web—the future realization of which is now often referred to as the “next generation network” or “NGN.”

Liberty's vision is to enable a networked world in which individuals and businesses can more easily conduct transactions while protecting the privacy and security of identity information. We see this as a key aspect of the next generation network in any applied environment and most powerfully represented in NHIN’s proposed vision.

Liberty's federated identity standards and business guidelines offer the flexible, secure and open infrastructure that is required to support and manage online services and transactions. We also believe that privacy, confidentiality and security, the core “deliverables” of Liberty’s specifications, should have a central role in the NHIN process and that a federated approach is critical to pervasive interoperability and real marketplace success.

¹ More information about the Liberty Alliance Project is available online at <http://www.projectliberty.org>.

It is in this capacity, and, with this collective expertise, that we have become engaged in the “Joint Filing” by Markle, HIMSS et al.; and it is from this substantive perspective our contribution should be understood. At various points in this document, our citation of “Joint Filing” refers to this multiparty collaboration.

Second, a number of Liberty members are directly involved in health care and have participated in legacy efforts to evolve integrated health information networks such as an EPR or other elements of the National Health Information Infrastructure (NHII) vision.

LAP members see their collective role as an enabler of interoperability. Fostering network interoperability is as germane to banking networks, distributed educational networks or air traffic control as it is to health care. But in the health care arena the stakes are particularly high. Health care is the largest employer expense after payroll; 35 million Americans have no health insurance or access to low cost providers. So there is enormously more to be gained by getting a savings-generating network deployed here than in any other market vertical.

Liberty believes that a “maximum” vision for NHIN should be pursued and that incremental approaches should be discouraged. While limited achievement of interoperability in regional health networks might be promising, it will not benefit all Americans and, in fact, may directly exclude communities that need improved health care the most.

To embrace less than a maximum vision is a disservice to the American people and will simply entrench parochial interests which pose barriers to true interoperability.

It is important to invest in difficult efforts, subordinate proprietary interests and acknowledge that there is more to be gained by acting together than by protecting our own institutional interests. That is why LAP members think it is important to raise a clarion call about the existence of this proceeding. Liberty is naturally concerned about the generally lukewarm level of interest about the RFI and the overall ONCHIT effort expressed by health industry journals and Web sites such as Medscape, eHealth or Google SciMed. And, where some discussion of EPR or eHealth does arise, it seems to reflect concerns regarding achievability that are unchallenged by any organized effort by ONCHIT. LAP and its members recognize that broad participation is critical for the overall success of this effort, and encourage ONCHIT to reach out to the wider community in ways that raise awareness and encourage participation by the widest communities of interest, beyond the health cognoscenti.

This issue of participation is critical. The LAP specifications are both open and non-proprietary, thereby enabling a wide variety of competitive, but interoperable, implementations and deployments. This permits a broad range of parties to participate in networks and to rapidly, accurately, and almost simultaneously achieve the authentications and exchanges necessary to engage in health care-related activities. Our specifications have been built to support this concept of secure participation across multiple platforms.

Liberty does not want this effort to represent a false start, but rather a promising beginning. This work has the potential to affect the quality of life of all Americans.

2. Responses to Questions

General

Question 1

The primary impetus for considering a NHIN is to achieve interoperability of health information technologies used in the mainstream delivery of health care in America. Please provide your working definition of a NHIN as completely as possible, particularly as it pertains to the information contained in or used by electronic health records. Please include key barriers to this interoperability that exist or are envisioned, and key enablers that exist or are envisioned. This description will allow reviewers of your submission to better interpret your responses to subsequent questions in this RFI regarding interoperability.

The NHIN should be understood as an “environment” or “ecosystem”. The technology “network” elements that will enable it are the Internet and the Next Generation Network (“NGN”) that is evolving from the convergence of the legacy Internet and other information pathways (such as the PSTN and wireless telephony).

The singular element of the National Health Information Infrastructure (NHII) that must be achieved is a disciplined conformance of all participants to a single specification for interoperability at the network transport level of constituent “sub-networks” (whether geographical, institutional, affinity or based on other organizing elements).

LAP’s unique value in this process is its articulation of non-proprietary specifications to achieve functional interoperability among the many and diverse “sub-networks.” This may be understood in IT jargon as the development and adoption of secure connectivity or “federation” with multiple industry implementations, and clear consolidation to a single foundation specification, with widely available commercial and open-source technology solutions implementing these specifications.

The HHS vision of the NHII is built upon the concept of “interoperability”. The concept is implicated in a number of the core components on which the NHII will depend (Common Framework, Standards and Policy Entity, Resource Locator Service), and is the condition that must be achieved by the NHII’s network elements, network participants, and data. Interoperability of technical platforms, interoperability of authentication régimes, and interoperability of data sets are all essential. While a variety of “definitions” for interoperability exist, it seems prudent to be as precise and comprehensive in suggesting the ways in which “interoperability” is crucial to the NHII.

As used in this filing, and as presented in the NHII "environment", INTEROPERABILITY has three distinct components, each of which must be present to enable full participation in the NHII:

1. at the information technology network level (here meaning the “Internet”) “Interoperability” means the capacity to physically connect a sub network user to the network for the purpose of exchanging data over its components with other NHIN participants and using that data;
2. at the network user and system authentication level (where the LAP SPECIFICATION IS MOST GERMANE TO THE NHIN by providing the specification for the standard by which parties and devices may authenticate themselves to the NHIN) “Interoperability” consists of the ability of a connected user to demonstrate appropriate permissions to participate in an instant transaction over the network, based on demonstrating prior attainment of appropriate authentication(s) of user and sub network identity as a privileged party; and,

3. at the application level, “Interoperability” means the capacity of a connected, authenticated user to usefully access, transmit and/or receive/exchange data with other NHIN participating users.

Question 2

What type of model could be needed to have a NHIN that: allows widely available access to information as it is produced and used across the health care continuum; enables interoperability and clinical health information exchange broadly across most/all HIT solutions; protects patients' individually-identifiable health information; and allows vendors and other technology partners to be able to use the NHIN in the pursuit of their business objectives? Please include considerations such as roles of various private- and public-sector entities in your response.

The classic IT model of packet switched network architecture (transport/routing/application) will be the backbone over which the NHIN will run. As a heterogeneous network—the “next generation network” (NGN)—it will necessarily have to conform ALL of its constituent transport, routing and signaling standards to generic network standards.

Virtually all NHIN objectives of interoperability, security, data integrity and privacy will emanate from generic network standards, as APPLIED in the NHIN application environments.

Quite simply, the concept of a “Common Framework,” (as set out more fully in the Joint Filing) articulating a disciplined specification, such as LAP's specification of a federated identity environment—becomes one—if not the—crucial mediating element in assuring interoperability of services and data exchange on the NHIN, while achieving such desired social benefits of privacy and confidentiality.

Question 3

What aspects of a NHIN could be national in scope (i.e., centralized commonality or controlled at the national level), versus those that are local or regional in scope (i.e., decentralized commonality or controlled at the regional level)? Please describe the roles of entities at those levels. (Note: “national” and “regional” are not meant to imply federal or local governments in this context.)

Within the healthcare industry, there's a legacy of competing views between "national" and "regional" elements of the NHIN architecture. This current structure is not helpful in understanding the necessity of uniform adherence to technical specifications or standards that enable interoperability. In a new more interoperable environment/world these specifications, above all else, must be “uniform”—or “national” in scope.

Uniformity at the interface between sub-networks and the underlying IT transport layer, further, lessens the competition between the "national" vs. the "regional" elements of architecture and enables integration of special-purpose networks with general enterprise and consumer services networks. It also maintains the analysis of “interoperability” with a focus toward achieving interoperability at the application level (for data exchange and use), and at the network authentication level for services supporting identity management as well as party and device authentication.

The Joint Filing's adoption of the concept of "sub-network"—in lieu of, but incorporating—"regional" is a crucial evolution in understanding how the components of NHIN will fit together.

Organizational and Business Framework

Question 4

What type of framework could be needed to develop, set policies and standards for, operate, and adopt a NHIN? Please describe the kinds of entities and stakeholders that could compose the framework and address the following components:

- a) How could a NHIN be developed? What could be key considerations in constructing a NHIN? What could be a feasible model for accomplishing its construction?
- b) How could policies and standards be set for the development, use and operation of a NHIN?
- c) How could the adoption and use of the NHIN be accelerated for the mainstream delivery of care?
- d) How could the NHIN be operated? What are key considerations in operating a NHIN?

Liberty strongly endorses the Joint Filing's development of the "Common Framework" approach as the operating predicate for the NHIN, permitting assurance of conformity with necessary specifications for interoperability, including sub-network conformity and interoperable authentication for parties and system participants. In conjunction with a record locator ability and a standards and policy mechanism, the essential operational requirements for open, interoperable participation by any sub-network will be enabled by the "Common Framework." Liberty's members, through their commercial offerings conforming to the open, non-proprietary LAP specifications, are the source of the key elements in these three network tools.

Question 7

What privacy and security considerations, including compliance with relevant rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), are implicated by the NHIN, and how could they be addressed?

As set out in the LAP Privacy and Security Best Practices whitepaper², the LAP specifications afford user communities ("circles of trust") great flexibility in achieving sector-specific objectives:

The Liberty Alliance considers privacy and security of a Principal's health-related personal information to be extremely important. Enabling world-class privacy protection and providing the ability to comply with HIPAA's privacy and security requirements are among the paramount differentiators between capabilities offered by LAP's specifications and other authentication capabilities presently available.

² Available at <http://projectliberty.org/about/whitepapers.php>.

Privacy and security considerations are fundamental to the Liberty Alliance framework. In particular, the Liberty Alliance made the following decisions regarding the Liberty specifications:

- To use a de-centralized architecture, where it is not necessary to have data stored with a single entity;
- To use a federated architecture, where parties are free to link networks as business judgment dictates;
- To support and promote permissions-based attribute sharing to enable consumer choice and control over the use and disclosure of his or her personal information;
- To provide open specifications that are not centrally administered;
- To provide interoperable specifications that can be used on a wide variety of network access devices;
- To leverage existing systems, standards, and protocols where they work well in order to preserve investment in legacy systems;
- To enable companies to transmit information using the specifications with the best available security;
- To include in the specifications, tools that enable companies to respond to consumer interests regarding privacy and security and to compete on that basis.

Question 8

How could the framework for a NHIN address public policy objectives for broad participation, responsiveness, open and non-proprietary interoperable infrastructure?

As stated in response to Question 2, LAP believes the concept of a “Common Framework”, articulating a disciplined specification, such as LAP’s specification of a non-proprietary federated identity environment becomes one—if not the—crucial mediating element in assuring interoperability of services and data exchange on the NHIN, while achieving such desired core “social” benefits as privacy and confidentiality. It also encourages broad participation by enabling multiple competitive implementations and deployments, while maintaining the goal of interoperability.

Management and Operational Considerations

Question 10

1. How could the NHIN be established to maintain a health information infrastructure that:
 - a) evolves appropriately from private investment;
 - b) is non-proprietary and available in the public domain;
 - c) achieves country-wide interoperability; and
 - d) fosters market innovation.

The same criteria for achieving interoperable applications that meet “performance requirements” for security, privacy and data integrity (see Q. 8) also should be incorporated in the basic specifications of standardized interfaces for application sets and constituent “networks” if these more fundamental objectives of an open NHIN, operating in an NGN environment, are to be assured. They are, however, part of virtually all working assumptions about transport and routing infrastructures of the NGN, and their relationship to the application, services and signaling layers that will run over them.

LAP’s specifications are prototypical of the characteristics necessary to assure that these functional objectives are met. Their incorporation as a “standard” would be consistent with the operating objectives articulated in the RFI, the NHII and the President’s Strategy.

The achievement of a special purpose network for health care information that meets the four conditions of Q. 10 (evolve from private investment; non-proprietary, fully interoperable, technologically dynamic) is an example of the objective for future applied networks of many other “market verticals”: i.e. securities, retail banking, and capital goods manufacturing.

Few have the societal implications of a health care network, but none, including health care, presents insurmountable barriers AT THE SYSTEM INFRASTRUCTURE level. Because these systems will depend on the evolving, open “Internet” and “next generation network” and because they will be developed in real time, evolve and be deployed by institutions with vested interests in their success, they will all be able to trace their architectures to extant technologies.

These are generic issues that Liberty has addressed with business use cases and guidelines which are meant to demonstrate adaptability of the Liberty specifications as generic “rules of the road” appropriate for any applied environment, including the NHIN.

Existing deployments and systems provide good models for essential components and operation. Among the most robust commercial systems running on the Internet is the credit card payment structure utilized by most of North American on-line merchants for their customers.

While the basic transaction is a simple barter, as many as a dozen institutions are implicated in the simple act of a customer providing a credit card number in a secure portal to a merchant.

What no party normally sees in this transaction are the almost instantaneous and simultaneous queries, reports and permissions reflected in the simple purchase, generated by any or all of the following:

- the selling merchant
- the purchasing customer
- the on-line site operator
- the customer’s bank
- the customer’s bank’s credit card processor
- the payment processing agent
- the selling merchant’s credit card processor
- the selling merchant’s bank

Leaving aside data issues and privacy/security requirements which may be added, the health care information environment is, generically, not very different from the on-line sale situation. Both share the need for rapid, accurate authentication of multiple parties, the accurate location of sensitive data, and the secure transmission of the data among custodial parties to third parties, with whom it may have no prior

contact, and for whom the mediation of permissions and authentications by the network may be the only interaction ever occurring.

The LAP specifications are both open and non-proprietary, thereby enabling a wide variety of competitive, but interoperable, implementations and deployments. This permits a broad range of parties to participate in networks and to rapidly, accurately, and almost simultaneously achieve the authentications and exchanges necessary to engage in commercial on-line sales of goods. The precisely identical elements necessary for a fully interoperable NHIN are available within the LAP specification.

The following scenario illustrates how the multiple demands for party and sub-network authentication are handled by a Liberty-enabled system. A simple clinical office encounter and ePrescribing scenario shows the number of desired authentications and data exchanges such an encounter implicates. The LAP-enabled version should demonstrate the essential role a specification for interoperable authentication of parties and devices will play in the NHIN.

Clinical scenario/Use case for Liberty specification in NHIN encounter

In a basic electronic prescribing system, clinicians review, enter, manage, and sign prescriptions using a computer, instead of writing them on paper. In addition to basic prescription entry capability, the definition of electronic prescribing includes a number of important capabilities, including:

- Clinical decision support, including alerts and reminders to promote guideline compliance, prevent prescribing errors, and advice about formulary compliance.
- Integration of other patient data from an electronic medical record, such as medical conditions, current and prior medications, allergies, laboratory results, and personal preferences, to enhance efficiency, improve documentation, and increase the potential impact of clinical decision support.
- Fax or electronic communication between clinicians, pharmacies, and health plans, in order to transmit prescriptions, conduct eligibility and benefit transactions, exchange messages, and process renewal requests.
- Provision of product information/educational materials for patients and clinicians.

Parties to the clinical encounter

Clinician, patient, payor, pharmacist, Directory Services, electronic prescription mediator.

ePrescribing Scenario	
NOTE: <i>Italics in the right column indicate an event mediated by a Liberty-specification based authentication or resource locator.</i>	
Without Liberty (or Another Interoperability Agent and Electronic Authentication Support)	With Liberty Support
1. Adam visits Dr. Jones's office. (Adam "authenticates" himself to practice clerical staff).	Adam visits Dr. Jones's office; <i>presents previously issued credentials</i> identifying him as: (1) an established patient; (2) ePrescription "client;" (3) an enrollee of payor "InsCo." Adam's credentials may support other permissions and privileges as well.

2.	Physician has access to Adam's paper medical record at Office Visit.	Using Liberty services, the physician has access to components of Adam's medical records (according to permissions and authority) <i>wherever they are located</i> , plus, possibly, Adam has given <i>permission to access various related histories</i> (personal, professional; self-recorded dairies), <i>preferences</i> (time-based, location-based), and <i>contextual resources</i> (level of emergency, etc).
3.	Dr. Jones diagnoses flu and prescribes appropriate medication.	Dr. Jones diagnoses flu and prescribes appropriate medication.
4.	Dr. Jones goes on-line and authenticates himself to ePrescription.com; he selects Adam from ePrescription's subscriber-patient list.	<p>Dr. Jones <i>accesses his practice's secure account at ePrescription</i> based on an <i>earlier authentication</i> he performed to his clinic intranet or device. His privileges at ePrescription could be constrained by: his licensing status, the role assigned to him by his clinic (relevant if he were only able to prescribe refills etc.) or his practice's participation with the payor.</p> <p>Dr. Jones's <i>query to ePrescription</i> displays a list of his eligible patients. The fact that Adam's name appears in the list may reflect a <i>prior explicit opt-in by Adam</i>. Dr. Jones selects Adam from patient list, confirming Adam's eligibility for this service.</p>
5.		ePrescription's system uses Adam's LAP-compliant Discovery Service for <i>resource location</i> , which supports determinations about where Adam's health records are maintained. Once determined, ePrescription uses an <i>opaque identifier (encrypted for the health records provider by the Discovery Service)</i> for Adam to generate a <i>query</i> (through a standardized interface) for the relevant information (e.g. interaction risks based on Adam's prescribing history, drug allergies). Of course, the health data is only released if ePrescription is an authorized requestor based on permissions established generically between ePrescription and the record locator service, and specifically by Adam, Dr. Jones, and Adam's payor for encounter-specific controls over record requests for Adam.
6.	ePrescription determines the allowed drugs for Adam (according to his plan), and then	ePrescription's system uses <i>Adam's Discovery Service to determine the location of the</i>

	transmits the list of allowed drugs back to Dr. Jones.	<p><i>appropriate formulary information for Adam. Once determined, ePrescription uses an opaque identifier (encrypted for the formulary provider by the Discovery Service) for Adam to query (through a standardized interface) the allowed drugs for Adam (according to his plan) and then presents the list of allowed drugs to Dr. Jones.</i></p> <p>[Each element of steps 4-6 may occur virtually and simultaneously, with the reports to the doctor of patient eligibility and formulary propriety being the two “clinical” outputs. An alternative scenario would eliminate the ePrescription provider, and establish direct communication between Dr. Jones and the pharmacy. When pharmacy, doctor and patient are all authenticated, the transaction (fulfillment of the prescription for pick up or for dispatch to patient's address by preferred transport) can proceed.]</p>
7.	Adam might have medical conditions unknown to ePrescription.com.	Dr. Jones selects drug(s) (<i>guided by system to ensure no adverse reactions</i>), specifies prescription details, and <i>submits prescription</i> .
8.	Dr. Jones needs to re-authenticate each time he wants to use ePrescription.com.	
9.	Dr. Jones selects the appropriate drug and specifies prescription details; he submits the prescription.	
10.	ePrescription submits the prescription to pharmacy, but Adam may have changed pharmacies.	ePrescription uses a <i>Discovery Service to determine where Adam's Pharmacy vendor is. Once determined, ePrescription submits the prescription to the appropriate pharmacy using a (different) opaque identifier for Adam.</i>
11.	Adam's insurance might not cover medications.	Pharmacy needs to clarify the prescription and uses <i>Dr. Jones's Discovery Service to find his LAP-compliant Interaction Service</i> . The pharmacy sends him an IM asking him to call. The confusion is cleared up. The prescription is filled.
12.		<i>Pharmacy uses Adam's Discovery Service to locate his LAP-compliant Personal Profile provider in order to find his address so that the prescription can be shipped to him.</i>

13.	Prescription is filled.		Prescription is shipped. Adam feels better faster.

Key differences

- Discovery Service enables more flexible model. Adam doesn't need to inform ePrescription if he changes his preferred pharmacy
- More distributed model—no assumption that ePrescription maintains Adam's health information.
- Leverages Web Services stack with extensible model for security, routing, etc.
- Use of different pseudonyms for patient between provider pairings protects individual privacy without the need for a unique identifier
- ePrescription can offer different clinicians differentiated prescribing privileges while placing burden of managing identities on home clinic/hospital.
- Liberty-enabled scenario accomplishes at least 18 separate background data exchanges, between 7 or more parties, but requiring only 5 “initiating” on-line queries.

Summary

Liberty's specifications can provide a standardized infrastructure of discovery as well as identity, privacy policy and message security for ePrescribing.

Standards and Policies to Achieve Interoperability

Question 14

What kinds of entity or entities could be needed to develop and diffuse interoperability standards and policies? What could be the characteristics of these entities? Do they exist today?

A wide range of IT sector bodies address standards and practices. Some, including the IETF have a long history of providing purely technical “standards” and have evolved into de facto standards development organizations for the Internet. With the rise of diverse industrial institutional reliance on Internet services, and the evolving recognition of interoperable authentication of parties and devices on the network as the sine qua non of true eCommerce, organizations which have the broadest support of technology vendors, infrastructure and network operators and user communities have developed to assure the promulgation of specifications and standards that reflect the broadest needs across all communities of network users from every discipline.

LAP has evolved to meet the marketplace demand for precisely the kind of entity envisioned in this question: a diffuser of interoperability standards, specifications and policies. From LAP's own description of its mission:

“The Liberty Alliance Project is an unincorporated, contract-based group of more than 150 companies and organizations from around the world. Liberty's objective is to create open, technical specifications that (i)

enable simplified sign-on through federated network identification on all current and emerging network access devices, and (ii) support and promote permissions-based attribute sharing to enable a user's choice and control over the use and disclosure of such Principal's personal information. Liberty anticipates that these specifications will expedite the growth of e-commerce because they are designed to increase consumer convenience and confidence and to provide businesses with new business and cost-saving opportunities."

Liberty envisions that organizations will implement the Liberty specifications in connection with their Web-based offerings. Because privacy is important in these contexts, the Liberty specifications include the necessary features and facilities to enable an implementing company to comply with its national privacy laws and regulations, or in the absence of law or regulation, best practice. Thus the Liberty specifications will enable companies to adhere to information practices that comply with those laws and regulations.

Liberty's vision is germane to the NHIN task. Our work product emanates from an organization with members from diverse places in the world of IT who have come together to achieve a common objective. As demand for federated identity and interoperability continues to increase, the Liberty specifications logically represent an essential element of the next generation network. The specifications permit the widest range of parties to participate in networks and to rapidly, accurately, and almost simultaneously achieve the authentications and exchanges necessary to engage in health care-related activities. .