



Nationwide and Regional Health Information Networks and Federated Identity for Authentication and HIPAA Compliance

Christina Stephan, MD
Co-Chair Liberty Alliance eHealth SIG
National Library of Medicine Health Informatics Fellow, University of Minnesota

The Liberty Consortium

Consortium of over 150 diverse member companies and organizations developing **open standards** that anyone can implement, addressing the “**whole issue**” of **identity**:

- Public Policy compliance
- Privacy
- Business requirements
- Interoperability conformance testing & certification

Vision:

A networked world in which **individuals, businesses, organizations** and institutions can more easily **interact and collaborate** with one another while respecting the **privacy and security** of shared identity information.



There are **more than 400 million**
Liberty-enabled identities and
clients world wide.

2005 estimate, source: Liberty Alliance

*The Liberty Alliance is the **ONLY** global body
working to define and drive open technology
standards, privacy and business guidelines for
federated identity management.*



Federated Identity in a Nutshell

What is network identity?

The role and importance of network identity management.

Federation: How it works

Federated Identity in the Healthcare Organization Setting

The evolution of network identity management

Identity Management Standards

Federated Identity Concepts

User's Network Identity

A network identity is
**a user's overall global
set of attributes**
constituting their various accounts



Attributes can include:

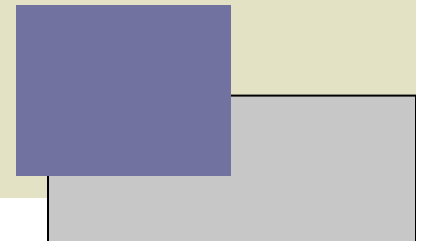
- User Name: John Smith
 - Email: jsmith2@freemail.com
 - PIN: 8822998
- Credit card number
 - Social security number
 - Drivers license
 - Passport
- Entertainment preferences
 - Notification preferences
 - Employee authorization
 - Business calendar
 - Dining preferences
 - Education history
 - Medical history
 - Financial assets...

Identity Impacts Everything

- Identity Impacts Everything-- including ***electronic health records and personal health records.***
- Identity is not an option, everyone and everything has an identity.
- Identity allows access to interactions in the health care environment and related transactions of value.

Identity Impacts Everything

- Identity Data is the information held about people, businesses and assets that enables those entities to be identified. This could include user ID, password, role, contact information, access rights and other account or user-related information.
- Identity Management is the effective management and leveraging of identity data. It involves a combination of technology, business process implementation and governance.
- An Identity Management architecture consists of a structural design for the IdM services, Identity data, underpinning technology and their relationships, consistent with the socio-political and business constraints.

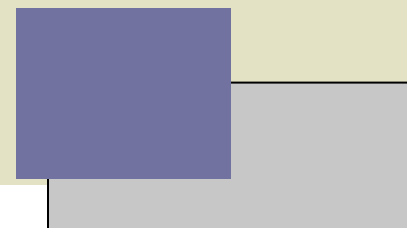


Identity Impacts Everything

- Identity and privacy has, at times, been compromised and/or placed at-risk.

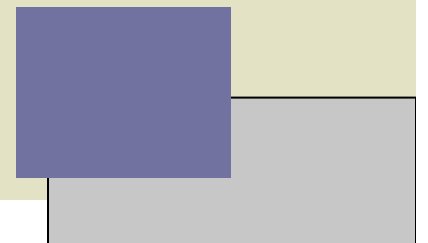
Challenges of protecting personal identity information and personal health information
Threatens the adoption of EHRs and PHRs as well as eCommerce growth.

- The result is a growing lack of trust, without trust, adoption of HIT and use of personal health information on the internet will be stymied.



Federation and Identity Management

- Federation is the way the world works today (drivers license, national ID, SIM cards...)
- Federation facilitates scalable, efficient, user-friendly, cross-domain Identity Management.
- Without Identity Management, federation fails...interactions and transactions become more difficult, if not impossible.
- Federation is a foundation for pseudonymous and anonymous secure business relationships.



The Importance of Identity

- Proper Identity Management makes a difference!
 - Fraud and Identity Theft prevention:
 - A distributed system can help, and so can the attribute and profile information sharing.
 - Secure and trusted usage and sharing of:
 - Personal Health Information and organizational identity information.
 - Personal Health and Financial information
 - Individual healthcare provider and organizational data for both remote and local intranet domain access



Evolution of Federated Network Identity

Separate Cards, Each Bank

Bank A
ATM Card

Bank B
ATM Card

Bank C
ATM Card

Linked Cards w/in Bank
Networks

Bank ATM
Network A

Bank ATM
Network B

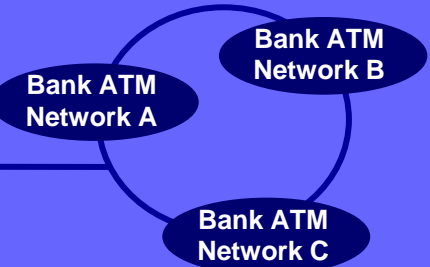
Bank ATM
Network C

Seamless Access
Across all Networks

Bank A
ATM Card

Bank B
ATM Card

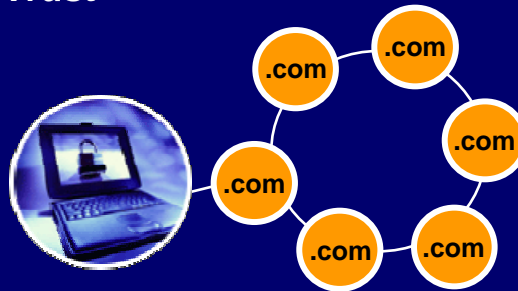
Bank C
ATM Card



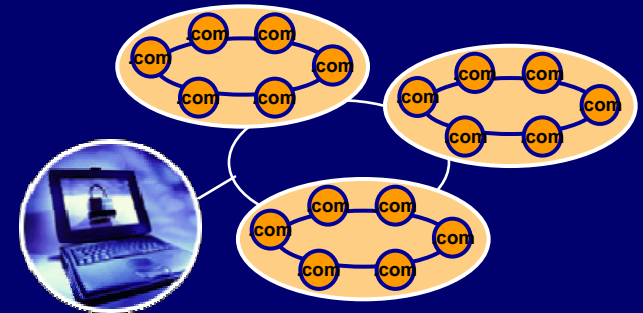
Individual Accounts with
Many Web Sites



Federated Accounts
within Circles of
Trust



Linkage of Circles of
Trust



Emergence and Convergence of Federated Identity Management (FIM) Standards


Organization	Standard(s)
OASIS (Organization for the Advancement of Structured Information Standards)	SAML: Security Assertion Markup Language; A standard language for making security assertions and attributes available in a federated setting.
The Liberty Alliance	ID-FF: Identity Federation Framework ID-WSF Identity Web Services Framework An open source federated identity standard with an emphasis on user privacy.
The Shibboleth Project	Shibboleth: A standard developed for use by academic institutions.
Microsoft, IBM	WS-Federation: A proposed web services standard, one of several such as WS-Security, WS-Authorization, WS-Privacy



Identity Management Terminology

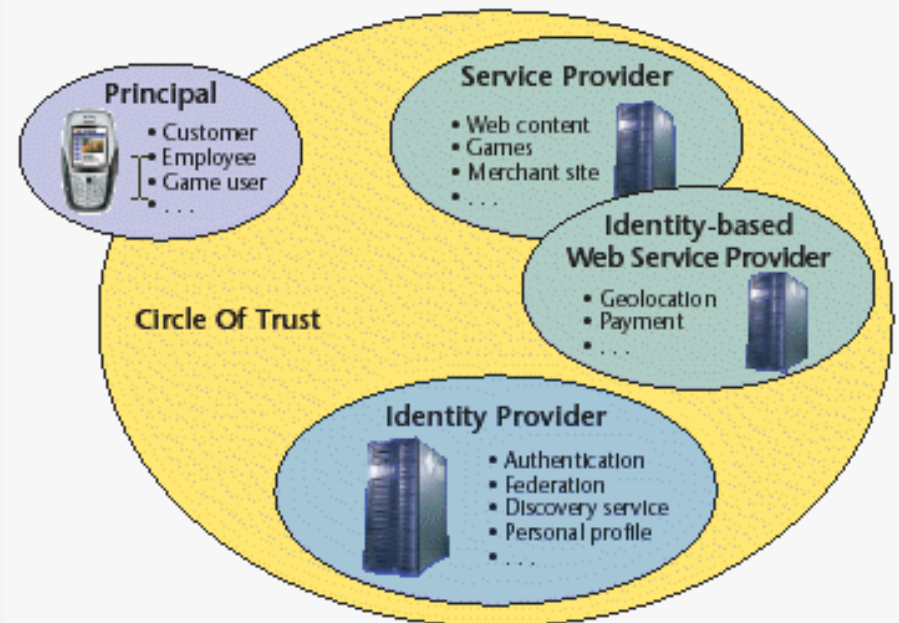
Key Concepts:

Principle, Identity Provider, Single Sign On
Services Provider, The Circle of Trust
Discovery Service



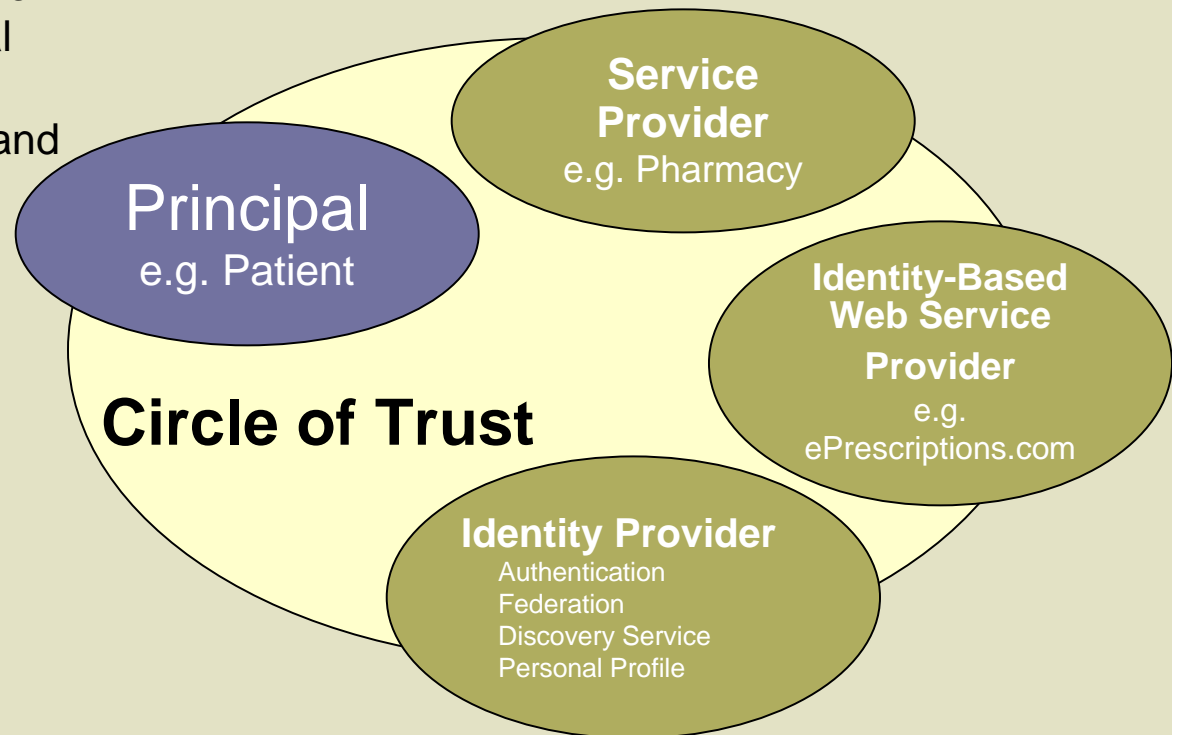
Key Concepts: I

- **Federation** – The act of establishing a relationship between two entities, an association comprising any number of Service Providers and Identity Providers.
- **Principal** – a person or “user”, a system entity whose identity can be authenticated.
- **IdP**, Identity Provider – a service which authenticates and asserts a Principal’s identity – usually the entry point into a Circle of Trust.
- **Single Sign-On (SSO)** – the Principal’s ability to authenticate with one system entity (Identity Provider) and have that authentication honored by other system entities, often Service Providers.



Federated Identity: Key Concepts: II

- **Circle of Trust** – a group of service providers and identity providers that have business relationships based on Liberty architecture and operational agreements and with whom users can transact business in a secure and apparently seamless environment. Circles of Trust represent the second wave of identity federation, after SSO and federated account linking.
- **DS** – Discovery Service – provides discovery of Identity-based Web Services.



Further definitions from the Glossary, found at: <http://www.projectliberty.org/specs/liberty-glossary-v1.3.pdf>



Federated Identity in the Healthcare Organization Setting

The Current Situation: Identity Silos

Identity Silos in Healthcare

There are many identity silos in healthcare
This impedes sharing of health information and has a negative impact on health care effectiveness.



Hospital Identity silo



Clinic Identity silo



Specialty care
Identity silo



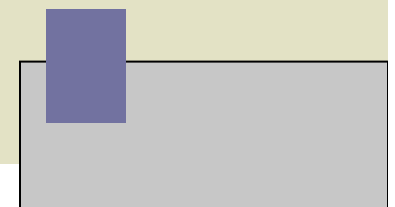
Administrative/payor
identity silo



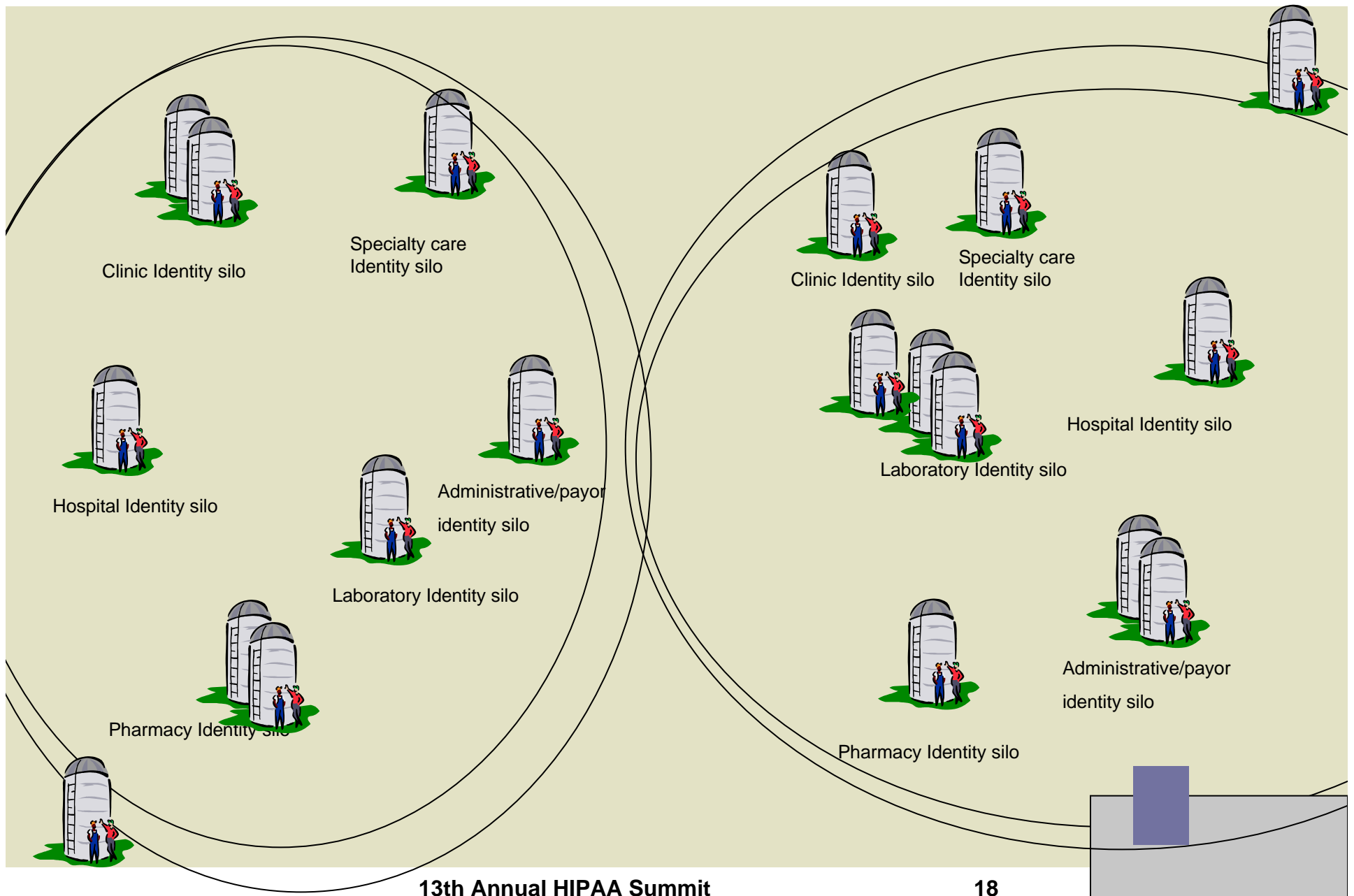
Pharmacy Identity silo



Laboratory Identity silo



Many duplicative Identity Silos in Healthcare



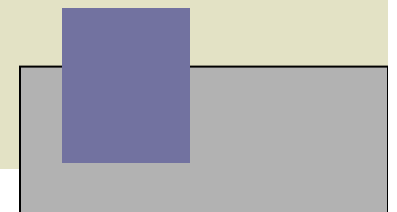


The Benefits of Federated Identity in Healthcare

Security:
Interoperability
Regulatory Compliance
Operational Efficiency
Cost Reduction

The Benefits of Federated Identity in Healthcare

Benefit	Examples
Security	<ul style="list-style-type: none">▪ User authentication:▪ Multiple access levels
HIPAA Compliance	<ul style="list-style-type: none">▪ Supports authentication levels▪ Enables detailed audit logs of records access
Improved Operational Efficiency	<ul style="list-style-type: none">▪ Single sign on▪ Management of UserID distinct from applications▪ Readily scalable to include new organizational participants
Cost Reduction/Avoidance	<ul style="list-style-type: none">▪ Support operations for identity administration▪ Decrease development time▪ Standards accelerate implementation-reduce need for disparate interfaces,
Interoperability	<ul style="list-style-type: none">▪ Allows integration of legacy systems▪ Eases new deployments,▪ Federated identity is more secure



Federated Identity and Health Care

Federated Identity Management “plumbing” standards that:

- Wide-spread adoption
- Convergence with other standards
- Federated authentication model
- Built on standards
- Privacy & security best practices
- Conformance testing & certification
- Provides for multi-product interoperability

Benefits of network technology without compromising security or control over Personal Health Information (PHI)

For Patients:

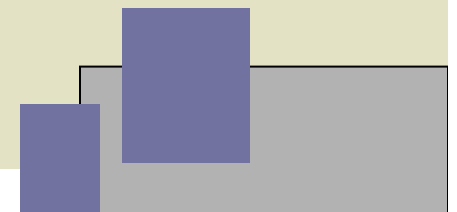


- Convenience of single sign-on
- More control over privacy and PHI
- Improved access
- Facilitates communication with providers & payers
- Improved patient trust and quality of care

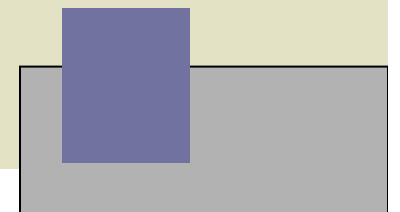
For Providers:



- Reduced medical errors
- Better and more services, new revenue opportunities
- Improved access
- Improved operating efficiencies
- Reduces IT costs
- Easier, faster HIPAA compliance
- Improved patient trust and quality of care



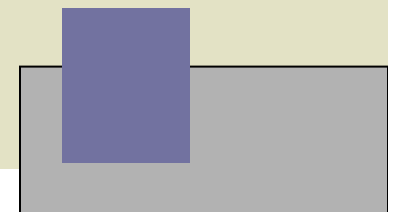
*Should Federated Identity management
be adopted in Healthcare?*



YES!

An Identity management Architecture will allow:

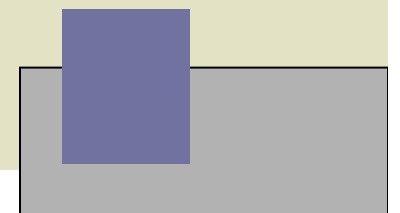
- Better privacy protection.
- More secure transactions involving personal health information.
- Regulatory compliance requires accurate complete access audit trails.



The adoption of Federated Identity in healthcare

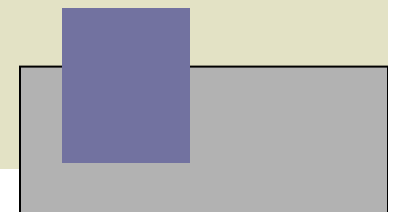
is NOT a TECHNOLOGY issue—

it is a POLICY issue...



So what are the barriers to adoption of Federated Identity?

- Some barriers include:
- Individuals, organizations, governments face risk of loss of privacy, loss of data integrity, loss/theft of identity.
- Currently, there is no coordinated government effort for identity management in healthcare.
- Chicken and egg scenario: Health care is delivered locally, but funding/payors are national organizations.



The Challenges

- **Trust** is implicitly legislated between government entities but does not mean it happens.
- **Multiple stakeholders** of different perspectives attitudes and objectives are involved.
- **Tension** between Federal and state and local and functional departments, or policy and operations.
- **No mandate** for use of specified architecture or standard (it's coming!).
- **Distributed governance** without centralization of authority.
- **Funding**: Who and how to finance, Governance: Who and how to govern?
- Currently **rare use** of cross boundary/enterprise services within healthcare.

What are the implications of delayed adoption of Federated Identity?

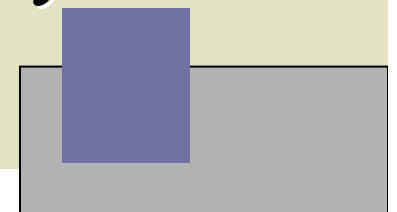
Higher per transaction costs with diminished return benefit use of web-based services.

For example, in the UK, only 5% of the population uses e-government based services:

- 34% of citizens polled indicated they would prefer not to use the internet for public services since it is not “secure”-
ICM Hedra 2002 (similar in the US)

- 57% of senior level civil servants believe security concerns are impeding the public adoption of web-based e-government services -*eGovernment Bulletin 2003*

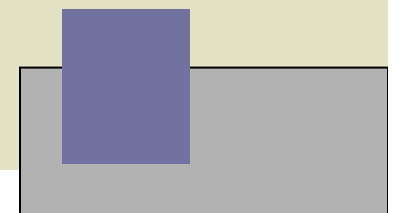
Identity theft has become a major issue globally.



So how do we

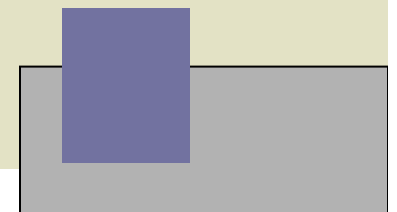
encourage adoption

of Federated Identity Management?



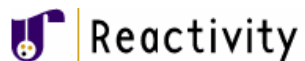
Fostering adoption of web-based services for healthcare...

- Create the next generation architecture which supports user privacy features and security.
- Existing systems should be leveraged to the greatest extent possible across health care—cannot afford to “rip and replace”.
- Foster adoption of collaborative working models which address inter organizational issues.
- Increase use of open standards.



Who is the Liberty Alliance?

- ~ 150 diverse member companies and organizations representing leaders in IT, mobility, government, service provision, system integration and finance from across the globe
- Management Board and Sponsor members include:



Call to Action: Join Us!

Liberty brings value to our Healthcare members:

- Federated Identity Management “plumbing” standards that:
 - Support key elements of NHIN interoperability
 - Make it much easier for patients, providers and payers to share results of authentication
 - Enable easier, faster HIPAA and other “best practice” compliance
- Conformance and compliance testing that assure base levels of interoperability and functionality

For more information:

https://www.projectliberty.org/resources/featured_verticals_health.php

Become Engaged:

✔ Visit us at the Interoperability Demonstration Project

✔ See the specifications and white papers at:
www.projectliberty.org

✔ Become a member!

