Liberty Alliance Workshop

April 26, 2006

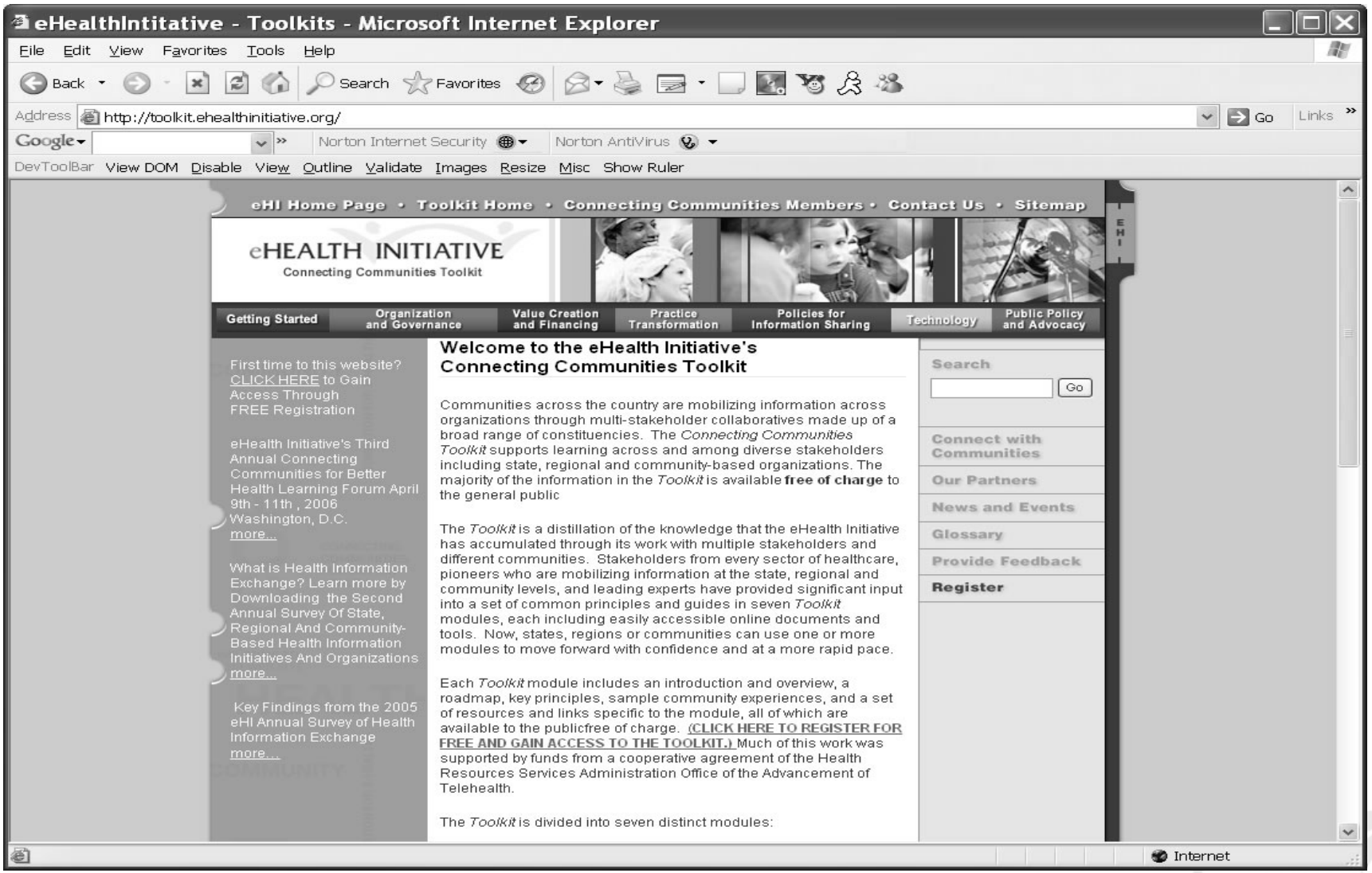
Security and Privacy

Leveraging Public-Private Partnerships

William R. “Bill” Braithwaite, MD, PhD, FACMI
Senior Vice President and Chief Medical Officer
eHealth Initiative and Foundation

eHEALTH INITIATIVE
Real Solutions, Better Health

Connecting Communities Toolkit - *Launched Jan 31, 2006*



eHI Toolkit for HIE

eHEALTH INITIATIVE
Connecting Communities Toolkit

Comprehensive on-line, interactive resource that walks the community through the seven critical components of success:

- Getting started: Assessing environment, engaging stakeholders, developing shared vision and goals
- Organization and governance, legal issues
- Value creation, financing and sustainability
- Policies for information sharing
- Practice transformation and quality improvement
- Technical implementation
- Public policy and advocacy

Common Principles and Policies for Information Sharing (e.g.)

- HIE requires trusted relationships
  - or data sources will not be willing to share the data they hold.
- Each participant in HIE must agree to follow certain information sharing policies and procedures.
  - agreement must be under contract.
  - must be minimum necessary and not impinge on local decisions unless absolutely necessary.
  - all agreement terms must be based on mutually agreed upon principles.

Privacy and Security

- Two of the most difficult areas are privacy and security.
- Reasons: misunderstanding, unfounded apprehension, or specific fears.
- ‘Privacy’ is also blamed when other causes are at work.
  - e.g., lack of trust or competitive instincts.
- All parties must learn about and understand underlying principles on which trust and consensus may be built.
- Experience of existing HIE efforts shows that this is an interactive process that cannot be rushed.
- Most efforts start off with something that everyone feels comfortable with;
  - typically the sharing of health information between healthcare providers for treatment purposes.

5 Common Principles of Fair Information Practices

- **Notice**
  - The existence and purpose of record-keeping systems must be known to the individuals whose data is contained therein.
- **Choice**
  - Information must be collected only with the knowledge and implicit or explicit permission of the subject, used only in ways relevant to the purpose for which the data was collected, and disclosed only with permission of the subject or in accordance with overriding legal authority (such as a public health law that requires reporting of a serious contagious disease).
- **Access**
  - Individuals must have the right to see records of information about them and to assure the quality of that information (accuracy, completeness, and timeliness). In healthcare, records are rarely deleted or replaced, but this principle implies that there is at least a due process for individuals to amend poor quality information about them.
- **Security**
  - Reasonable safeguards must be in place for the confidentiality, integrity, and availability of information.
- **Enforcement**
  - Violations must result in reasonable and consistently applied penalties to deter violators and in reasonable mitigation efforts to offset the effects of a breach as much as possible.

Context of Privacy Principles in HIE

- It is important to adopt such a set of principles and constantly refer back to them when making decisions about health information sharing policies and procedures.
- Everyone involved must buy into the principles you choose to work with and be thoroughly familiar with them, their effect on the agreements that must be made, and the consensus that must be reached before a community is able to implement health information exchange.

Security Principles

- You cannot have privacy (or confidentiality of private information) without security measures to protect the information from being used or disclosed in ways that violate the other principles.
- The most confidential information is that which is secured in such a way that no one but the originator can access it.
  - in healthcare such information must be available when and where needed to improve clinical decision making about the subject.
- Characteristics of confidentiality, integrity, and availability are the backbone of health information security.
- To support all three, security must be implemented as a careful balance of administrative, technical, and physical safeguards which are tailored to the particular information systems environment of each installation.

Recommended Approach

- This is best done through a risk assessment of the information systems environment followed by ongoing risk management through the selection, implementation, and monitoring of reasonable and appropriate measures to minimize the risks while controlling the costs.
  - flexible and scalable approach is the basis for the HIPAA security rule, taken because security threats and solutions evolve too quickly to be writ in stone (as it were) in the form of federal regulation.
- Often, these measures involve policies, procedures, and contracts with business associates more than technology.
  - the majority of security breaches are from the ‘inside’, and for security technology to work, behavioral safeguards must be established and enforced.
  - requires administration commitment and responsibility at the highest executive level in an organization.

Security Nut Shell

- In a nut shell, security is the implementation of reasonable and appropriate administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of electronic health information.
  - Since security is such an important and visible aspect of HIE programs, it is important to identify and make known the person responsible for the development and implementation of the policies and procedures as well as the implementation and ongoing maintenance of security measures for the HIE.
- The HIPAA rule provides good general guidelines for health information security, but there are a few areas that should be emphasized for HIE projects which may be different based on the goal and implementation technology of the project.
  - For example, if the HIE is simply to serve as a conduit between participants without access to the content, then the security aspects are much simpler than if the HIE is holding copies of the clinical data and responding to queries on behalf of the data sources.

Security for HIE

- In general, particular attention must be paid to the following areas of security when designing the policies, procedures, and agreements for HIE:
  - User identification and authentication.
  - User authorization.
  - Role based access control.
  - Transmission security.
  - Minimum necessary.
  - Audit trail and information system activity review.
  - Response to security incidents and breaches
    - including reporting, sanctions, and mitigation.

Organizational Challenge: Multi-level, Multi-stakeholder, Multi-institution, Multi-Lateral Agreements

- Outside the purely technical realm, the most difficult problems involve getting consensus or agreement across all the institutions that propose to exchange health information.
  - They all have to agree at the high level principles level, at the nationwide policies and procedures level, and at the local, regional level of implementation.
  - All these levels of agreement must be committed to in contract language, a model for which is found in the Connecting for Health Common Framework …

What is Connecting for Health?

- Broad-based, public-private collaborative of more than 100 diverse stakeholders
- Founded and supported by **Markle Foundation**, with additional support from **Robert Wood Johnson Foundation**
- **Purpose of Connecting for Health:**

  To catalyze changes on a national basis to create an interconnected, electronic health information infrastructure to support better health and healthcare

Connecting for Health Prototype Goals

- Develop a policy and technical framework that enables information sharing to happen for high quality patient care while protecting the privacy and security of personal health information.
  - Identify what needs to be common for interoperability and what does not.
  - Design and develop the documentation and the materials for communities on issues such as access, control, privacy, and security.

What is the Common Framework?

- A secure nationwide health information exchange network will be enabled by the general adoption of a set of specific, critical tools including:
  - technical standards for exchanging clinical information,
  - explicit policies for how information is handled, and
  - uniform methods for linking information accurately and securely.

The Common Framework Design Principles

- Designed to safeguard privacy—imposed the requirement first and then designed the functional architecture
  - This approach is harder and requires resisting “if only” thinking.
  - It does not produce the easiest or simplest technical solutions
  - You can’t build first and worry about the policies later…

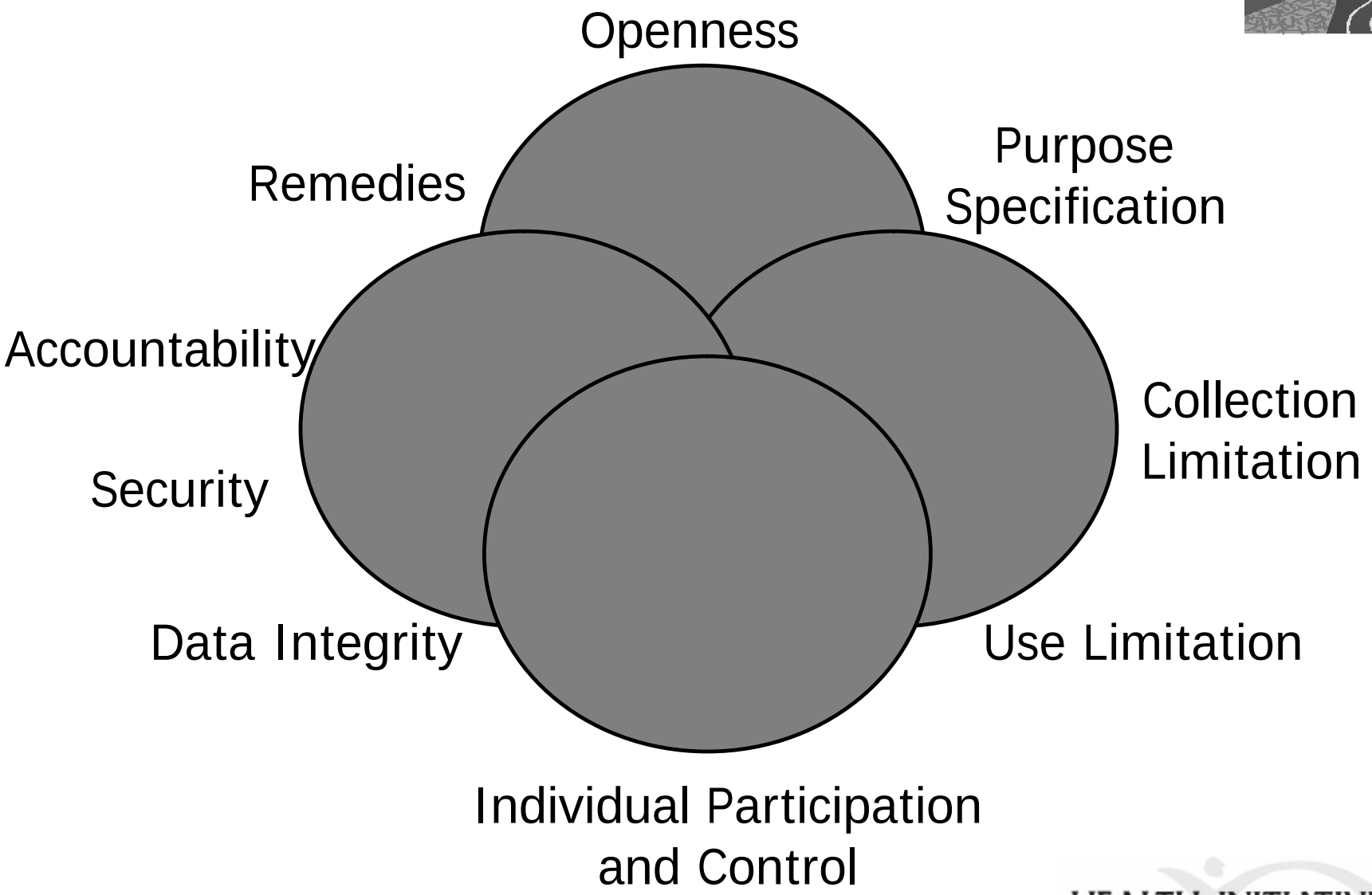
Who Developed the Prototype and the Common Framework?

- Connecting for Health Steering Group
- Policy Subcommittee: Co-Chairs Bill Braithwaite and Mark Frisse
- Technical Subcommittee: Chair: Clay Shirky
- Three communities and teams:
  - **Boston**: MA-SHARE and technical partner CSC
  - **Indianapolis**: Regenstrief Institute and Indianapolis Health Information Exchange (IHIE)
  - **Mendocino**: Mendocino HRE and technical partner Browsersoft, Inc.

Connecting for Health:
Policy Principles

1. Openness and Transparency
2. Purpose Specification and Minimization
3. Collection Limitation
4. Use Limitation
5. Individual Participation and Control
6. Data Integrity and Quality
7. Security Safeguards and Controls
8. Accountability and Oversight
9. Remedies

Connecting for Health: Policy Principles



Connecting for Health:
Technology Principles

1. Make it “Thin”
2. Avoid “Rip and Replace”
3. Separate Applications from the Network
4. Decentralization
5. Federation
6. Flexibility
7. Privacy and Security
8. Accuracy

The Common Framework: Overview and Principles

Policy Guides: How Information is Protected

- P1 — The Architecture for Privacy in a Networked Health Information Environment
- P2 — Model Privacy Policies and Procedures for Health Information Exchange
- P3 — Notification and Consent When Using a Record Locator Service
- P4 — Correctly Matching Patients with Their Records
- P5 — Authentication of System Users
- P6 — Patients' Access to Their Own Health Information
- P7 — Auditing Access to and Use of a Health Information Exchange
- P8 — Breaches of Confidential Health Information
- *Future Policy Guides*

Technical Guides: How Information is Exchanged

- T1 — The Common Framework: Technical Issues and Requirements for Implementation
- T2 — Health Information Exchange: Architecture Implementation Guide
- T3 — Medication History Standards
- T4 — Laboratory Results Standards
- T5 — Background Issues on Data Quality
- T6 — Record Locator Service: Technical Background from the Massachusetts Prototype Community
- *Future Technical Guides*

Model Contractual Language

- M1 — Key Topics in a Model Contract for Health Information Exchange
- M2 — A Model Contract for Health Information Exchange

P5: Authentication of System Users

- Identity (Who am I?)
- Identifiers (How is that Identity represented?)
- Authentication (How can I prove who I am?)
- Authorization (What can I do when I've proved who I am?)

P5: Authentication of System Users

- Requirements
  - Transitive trust, often based in contract
  - SNO must have identifiers for all participating entities
  - Users must be authenticated before given access to any SNO-wide resource containing patient data
  - Any request for data from a remote institution must have two pieces of identifying information (institution authenticating user and identifier for user)

P5: Authentication of System Users

- Requirements
  - "Break the Glass" function may be allowed (although not allowed in Record Locator Service itself)
    - Must be accompanied by description of rationale for request
    - Must be accompanied by an identifier for the user.
      - No "Emergency" account (role without identifier)
    - Requires timely human review and enhanced auditing

P5: Authentication of System Users

- Requirements
  - For patient to access his or her own records, initial access must be provided by participating institution or third-party recognized by SNO

The Common Framework Resources

- All materials available without charge at www.connectingforhealth.org
- Software code available from regional sites: Regenstrief, MAShare, OpenHRE

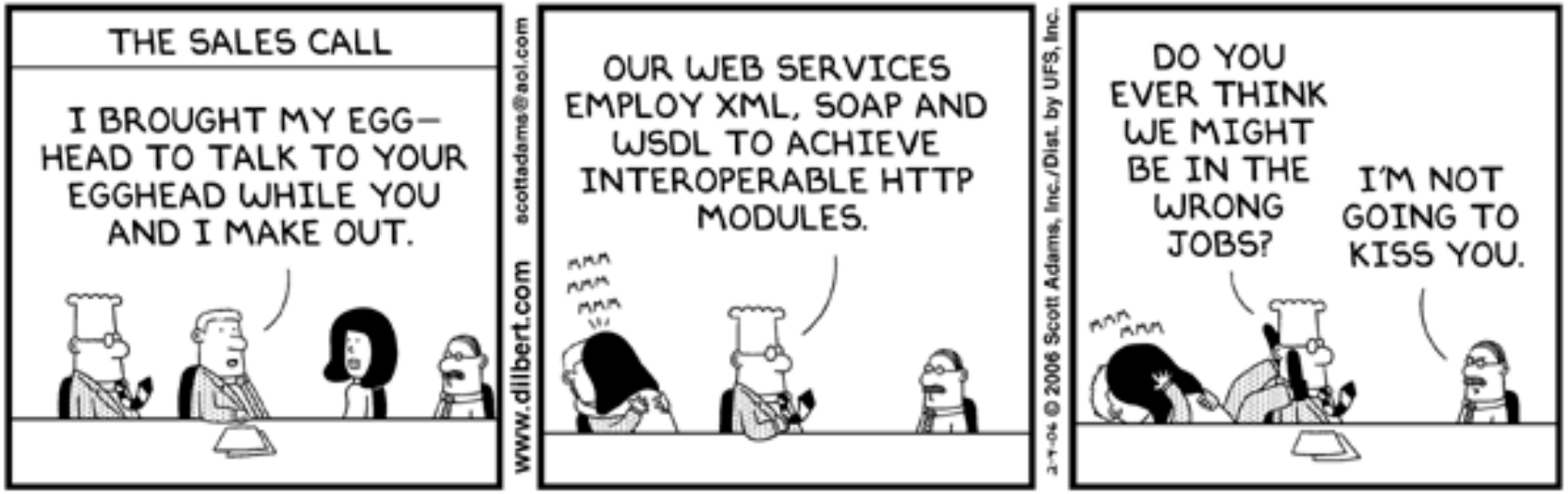
Technical Vision of HIE

- Network through which all authenticated participants may exchange information without loss of meaning:
- All message senders and receivers are authorized and authenticated.
- All messages are signed and encrypted.
- All messages are actively acknowledged or rejected by the receiver in real time.
- All messages meet conformance tests for use case specific standards that can support the exchange of clinical information between disparate information systems capable of different levels of interoperability.
- All information is exchanged in accordance with a set of principles, policies, and procedures to which each participant has agreed in a binding contract. The contract explicitly lays out the privacy, security, technical, and business rules that govern participation in the HIE.

Common Problem Space

- Requires a ubiquitous, secure, available, cheap communications infrastructure for healthcare.
- Can be used for administrative as well as clinical data exchanges.
- One major hurdle in implementation:
  - Trusted user identification, authentication, and authorization mechanism.

Something for everyone…



© Scott Adams, Inc./Dist. by UFS, Inc.

William R. “Bill” Braithwaite, MD, PhD, FACMI
Senior Vice President and Chief Medical Officer
eHealth Initiative and Foundation

www.ehealthinitiative.org
818Connecticute Avenue, NW, Suite 500
Washington, D.C. 20006
202.624.3270
Bill.Braithwaite@ehealthinitiative.org