EQUIFAX®

Identity: The Key to the Future of Healthcare

William R. “Bill” Braithwaite, MD, PhD, FACMI, FHL7
Chief Medical Officer
Anakam Identity Services

July 14, 2011

Why is Health Information Technology Critical?

- Avoids medical errors.
  - Up to 98,000 avoidable hospital deaths due to medical errors every year.
- Avoids healthcare waste.
  - Up to $300B per year on treatments with no health yield.
  - We spend 2X per capita as any other industrialized nation.
  - We rank last in population health status.
- Accelerates health knowledge diffusion.
  - Average of 17 years for medical evidence to be integrated into practice.
- Reduces variability in delivery and access.
  - Access to specialty care is highly dependent on geography.

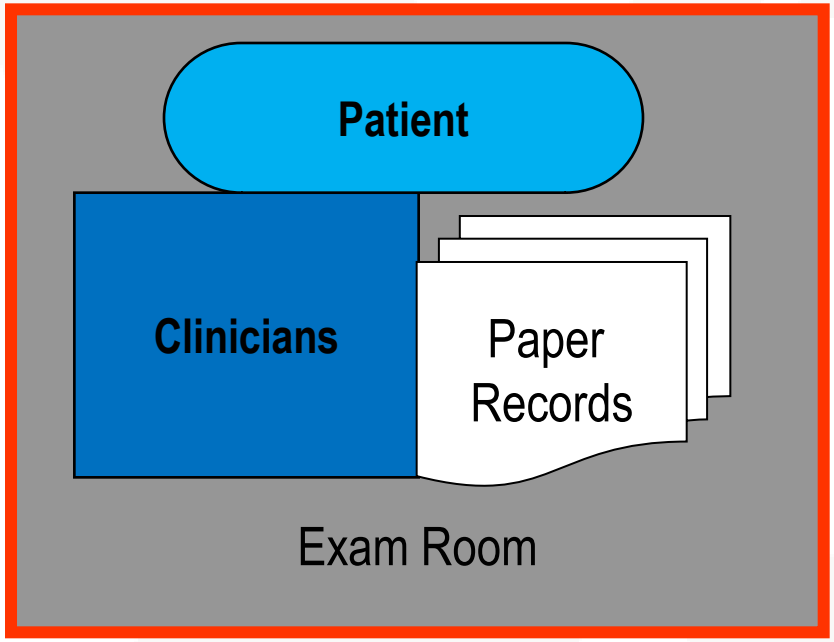
Why is Health Information Technology Critical?

- Promotes public health and preparedness.
  - Surveillance is fragmented, and untimely.
- Empowers consumer involvement in health management.
  - Patients currently minimally involved in own health decisions.
- Strengthens health data privacy and protection.
  - Public fear of identity theft and loss of privacy.

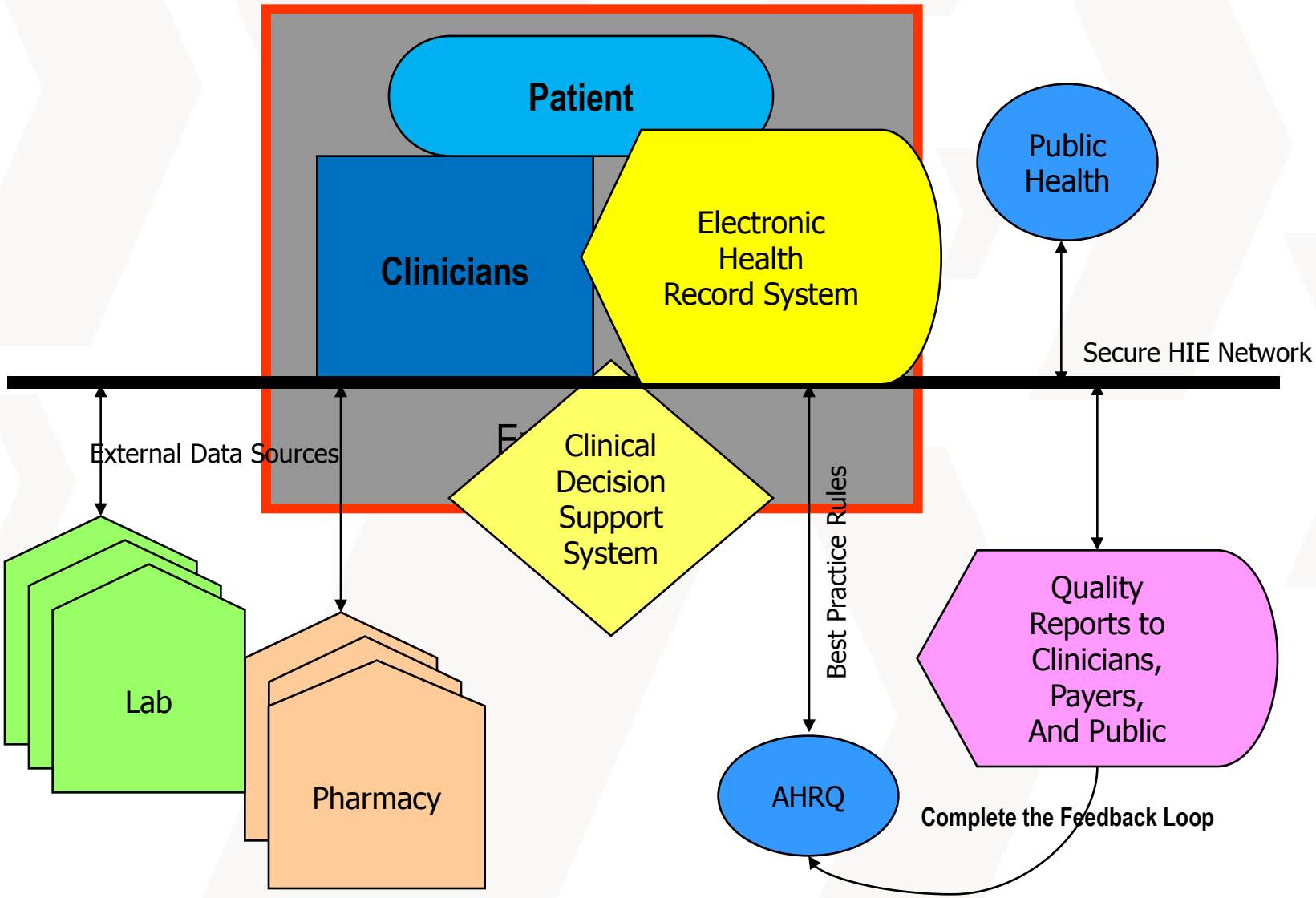
Healthcare Reform cannot do this without HIT.

- Paper records cannot solve these problems!

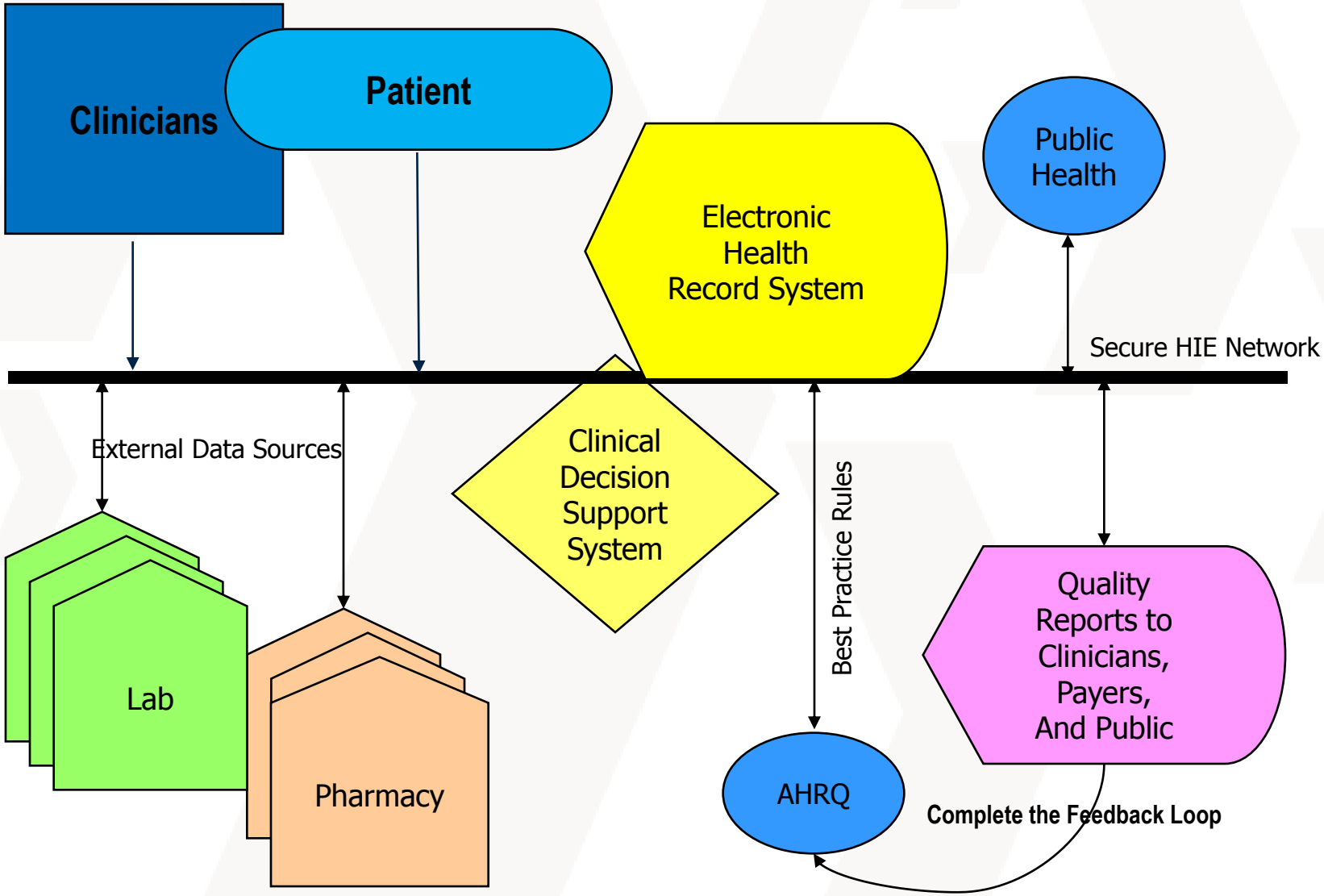
Evolution of Healthcare Paradigm



Evolution of Healthcare Paradigm



Evolution of Healthcare Paradigm



Future for Healthcare

- **Goal:** High quality, cost-effective healthcare.
- **Means:** Clinician/Patient direct interaction with Clinical Decision Support System (CDSS) (“Meaningful Use”).
- **Drivers:** HIE + EHR + CDSS => SAVES LIVES and $$$
  - Interoperable HIE is KEY to Meaningful Use of HIT which, in turn, is KEY to health reform!
- **Requires:** EHR (with CDSS and HIE) and:
  - Interoperability with sources of clinical data and sources of computable rules for best clinical practices (Standards).
  - Incentives to incorporate into healthcare practice (Resources).
  - Investigations of systemic failures to enable systems that detect and prevent errors through best practices at the point of decision making.
  - Trust through agreement on standards for interoperable security and privacy (including patient consent).

Trust

- Patients must trust the HIE system.
  - Lack of trust = no permission to disclose health records.
- Providers must trust the HIE system.
  - Lack of trust = no information exchange.
- Loss of perceived control of PHI in HIE.
  - Trusted provider no longer in charge of data.
- Access to large amounts of PHI accumulated by HIE.
  - Increased potential for breach which could stop HIE.

- **HIE will fail without access to PHI.**
  - **Health reform will fail without HIE!**

Trust depends on believable security mechanisms and a clean track record …

Security Requires Assurance of Identity

- High level of assurance that the person who is sending information is who say they are.
  - Message non-repudiation through electronic signatures.
- High level of assurance that the person who is receiving information is who we think they are.
  - Including mechanisms to prevent information from being changed or viewed by anyone else through encryption.
- High level of assurance that the patient identified in the information is who we think they are.
  - Patient identification accuracy.
- These mechanisms are dependent on high assurance identity proofing and multi-factor authentication.
  - NIST Level 3 assurance now available commercially at reasonable prices.

Assurance of Patient Identity

- No national standard for how to uniquely identify patients.
  - HIPAA requirement for standard patient ID was not implemented.
- Merging records from multiple locations is required.
  - Matching probability is much less than100% -- worse without SSN!
- Identity proofing of patients is required for security.
  - In-person identity proofing is impractical -- Providers don't want the job.
- Electronic access to medical records must be secured.
  - Internet access to patient portal is needed to meet consumer engagement goal of 'Meaningful Use'.
- Fraud prevention in public programs (e.g., Medicare and Medicaid) requires patient identity to be assured.
- Electronic recording of consent directives.
  - Must be assured that it is truly the patient who is setting the limits.

Assurance of Provider Identity

- Remote access to patient information (HIPAA).
  - Access from home, wireless devices, and patient homes.
- Access to government held PII.
  - OMB,FISMA, and NIST requirements.
- Submission of quality information.
  - Pay for performance programs.
  - Meaningful Use incentive programs (CMS).
- Fraud prevention and enforcement.
  - CMS (Medicare and Medicaid requirements).
- Electronic prescribing of controlled substances.
  - DEA requirements are very strict.

DEA IFR for Controlled eRx

- Only a DEA registrant may sign the prescription.
  - DEA regulation effective June 1, 2010.
- To sign, the registrant must complete a two-factor authentication protocol that meets the requirements of NIST Assurance Level 3 and uses two of the following three factors:
  - (1) Something only the practitioner knows, such as a password or response to a challenge question.
  - (2) Something the practitioner is, biometric data such as a fingerprint or iris scan.
  - (3) Something the practitioner has, a device separate from the computer to which the practitioner is gaining access.
- To obtain an authentication credential the registrant must pass identity proofing that meets the requirements of NIST Assurance Level 3.

The Problem:

- Identities are difficult to verify over the internet.
- Privacy remains a challenge.
- Numerous government services must be conducted in person or by mail, leading to continual rising costs for state, local and federal governments.

"On the Internet, nobody knows you're a dog."

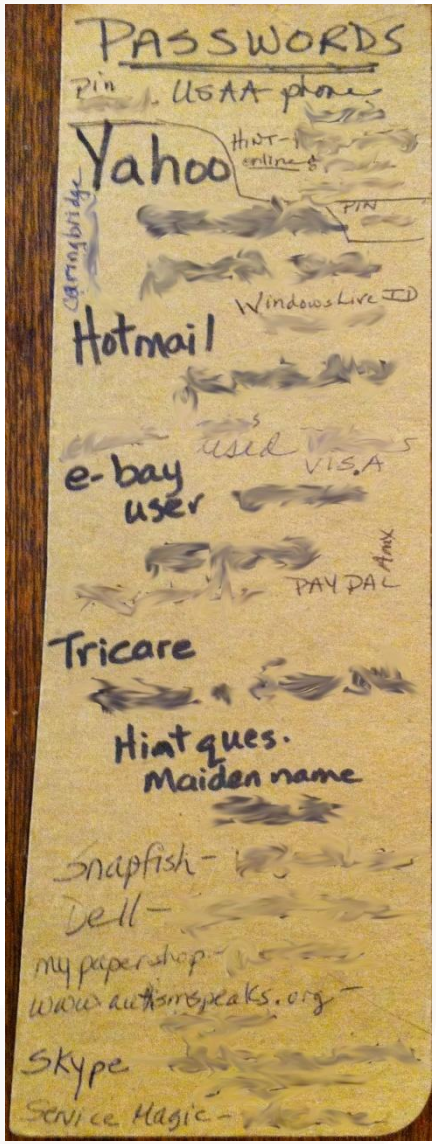
New Yorker, July 5, 1993

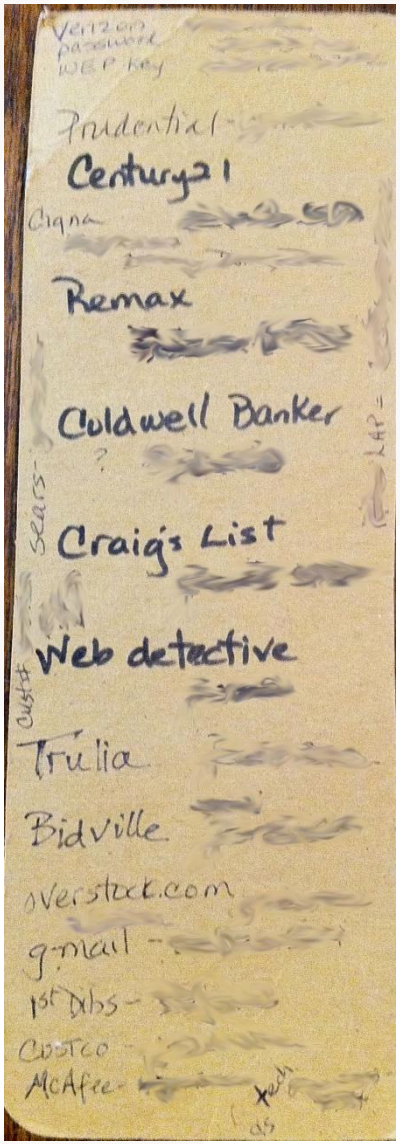
- **Electronic health records could save billions, but can't move forward without solving authentication challenge for providers and individuals.**

Usernames and Passwords are Broken

- Most people have 25 different passwords, or use the same one over and over.
- Even strong passwords are vulnerable…criminals can get the “keys to the kingdom”.
- Rising costs of identity theft.
  - 123% increase in financial institution Suspicious Activity Reports in last 6 years
  - 11.7 million est. victims over 2 years
  - $17.3 billion est. cost to economy over 2 years
- Cybercrime is also on the rise
  - Incidents up 22% from 2009 to 2008
  - Total loss from these incidents up 111%, to $560 million.

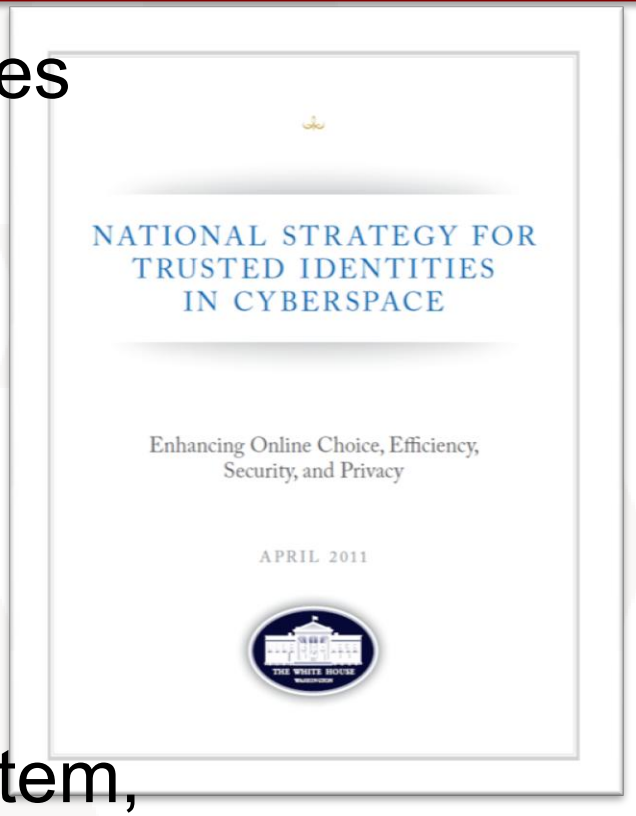
This is NOT the solution!





National Strategy for Trusted Identities in Cyberspace

- April 2011 NSTIC Guiding Principles
  - Privacy-Enhancing and Voluntary
  - Secure and Resilient
  - Interoperable
  - Cost-Effective and Easy To Use



- NSTIC calls for an Identity Ecosystem, "an online environment where individuals and organizations will be able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities."

NSTIC calls for:

- **Private sector will lead the effort**
  - Not a government-run identity program
  - Industry is in the best position to drive technologies and solutions
  - Can identify what barriers need to be overcome
- **Federal government will provide support**
  - Help develop a private-sector led governance model
  - Facilitate and lead development of interoperable standards
  - Provide clarity on national policy and legal framework around liability and privacy
  - Act as an early adopter to stimulate demand

Next Steps for NSTIC

- **Convene Private Sector** Workshops on governance, privacy and technology
- **FY11 Focus**
  - Establish Governance model
    - Private sector led; multi-stakeholder collaboration
    - Enable expedited focus on consensus standards and operating rules
    - Explore models for addressing liability
  - Design Pilots:
    - Develop criteria for selection
    - Assess potential programs
    - Prepare for formal pilot launches with funding in FY12
- **Government as an early adopter to stimulate demand**
  - Ensure government-wide alignment with the Federal Identity, Credential, and Access Management (FICAM) Roadmap
  - Increased adoption of Trust Framework Providers (TFP)

NIST IR 7497 -- TABLE OF CONTENTS

- **Security Architecture Design Process for Health Information Exchanges (HIEs) – September 2010**
  - 1.0 EXECUTIVE SUMMARY
  - 2.0 INTRODUCTION
  - 3.0 HIE CONTEXTS
  - 4.0 HIE SECURITY ARCHITECTURE DESIGN PROCESS
  - 5.0 CAPSTONE POLICIES
  - **6.0 ENABLING SERVICES**
  - 7.0 ENABLING PROCESSES
  - 8.0 NOTIONAL ARCHITECTURE
  - 9.0 TECHNOLOGY SOLUTIONS AND STANDARDS
  - 10.0 BUILDING A NATIONWIDE HIE USING REGIONAL HIES

ENABLING SERVICES

- Risk Assessment
- Entity Identity Assertion (Authentication) *
- Credential Management (Licenses, etc.) *
- Access Control (Authorization) *
- Privilege Management (Roles, Permissions) *
- Collect and Communicate Audit Trail
- Document Integrity (Hash and Electronic Signature) *
- Secured Communication Channel
- Document Confidentiality (Encryption) *
- De-identification
- Non-Repudiation of Origin (Electronic Signature) *
- Manage Consent Directives (Assured Patient Identity) *

•Identity Dependent Services

(8 of 12)

Anakam's Full Range of Identity Services

- Registration – Data Collection and/or Integration
- Identity Proofing – Record Matching / Identity Cleanup
  - Entity Proofing + association with responsible individual(s)
  - Individual Proofing = carbon-based life form, species homo sapiens
- Electronic Identity Tokens and Processes
  - Electronic Signature, PKI Keys, Authentication Tokens
  - Hashing, Encrypting, Signing, and Authenticating Documents
- Attribute Associations
  - Credentials (Licenses, privileges, etc.)
- Identity Authentication – multiple levels and methods available
  - High Level of Assurance (NIST Level 3) Required for PHI
  - Flexibility of multiple channels for multi-factor authentication
- Change Management

Anakam's Identity Management Solutions

- SECURE - allows full compliance with NIST Level 3
- SCALABLE - deployable to tens of millions of users
- TRUSTED - uniquely identifies users and helps prevent fraud
- FLEXIBLE - progressive authentication adapts to risk level
- COMPREHENSIVE - solves complex identity lifecycle challenges
- RISK BASED - tailored to enterprise use case and business needs
- EASY TO DEPLOY - installs inside your firewall or in the cloud

CONTACT

William R. “Bill” Braithwaite, MD, PhD, FACMI, FHL7
Chief Medical Officer
Anakam Identity Services
Equifax

Bill.Braithwaite@Equifax.com