

**DOCUMENT 2:
FUNDAMENTALS OF THE ELECTRONIC MEDICAL RECORD**

Fundamentals of the Electronic Medical Record



Case History:
Health Information Institute
("H2I")
<http://www.h2i.com>

Health Information Institute

Immunization Database System

- *Background:*
 - Centers for Disease Control
 - All Kids Count
 - Other Initiatives
- *Problems: Lack of Funding, Lack of Trust*

The Issue

In the U.S. each year:

- 30 million pediatric immunizations missed
- Avoidable deaths and costly complications
- 10 million immunizations duplicated
- Millions wasted in the paper chase
- \$10 M + wasted controlling avoidable outbreaks

Why?



Needed information not available:

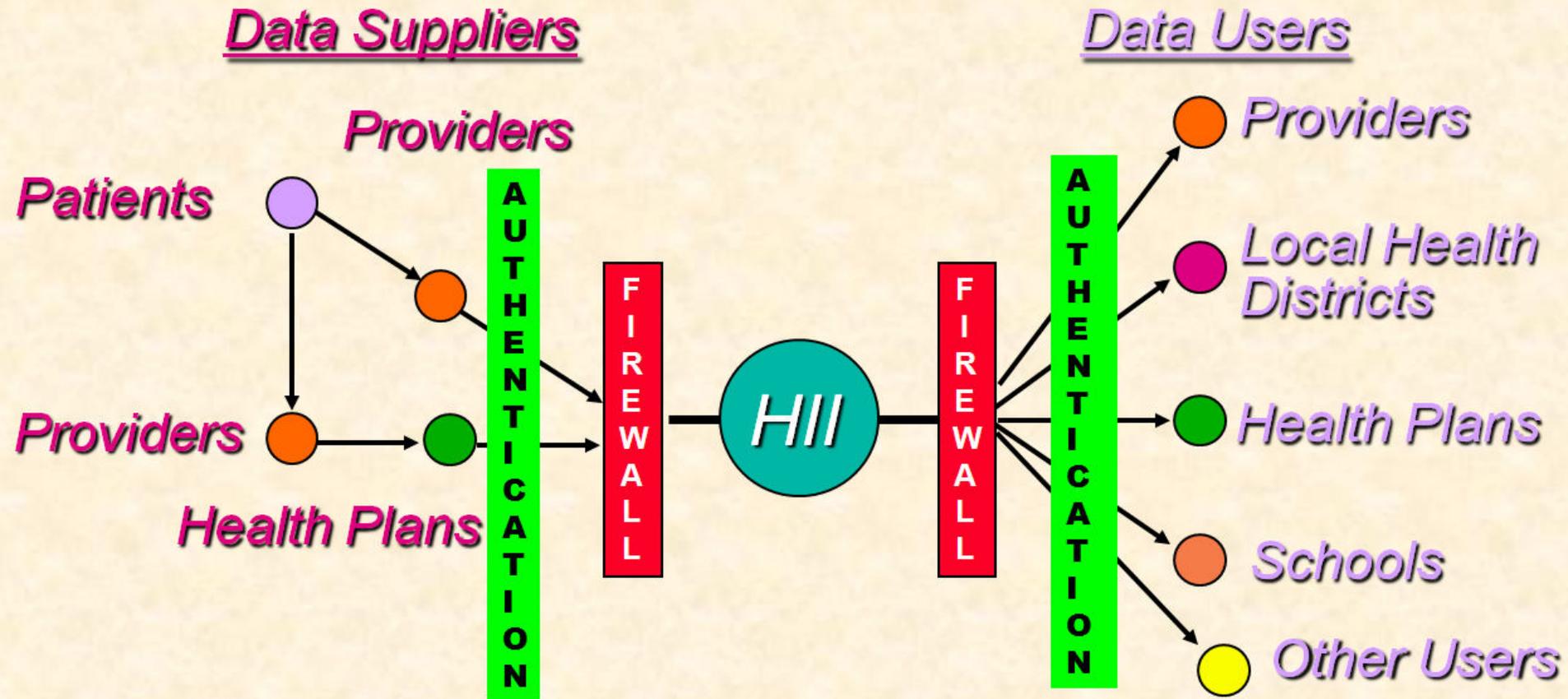
- Families change doctors frequently
- Parents do not have records
- Immunization requirements change
- Administrative cost of finding data

H2I

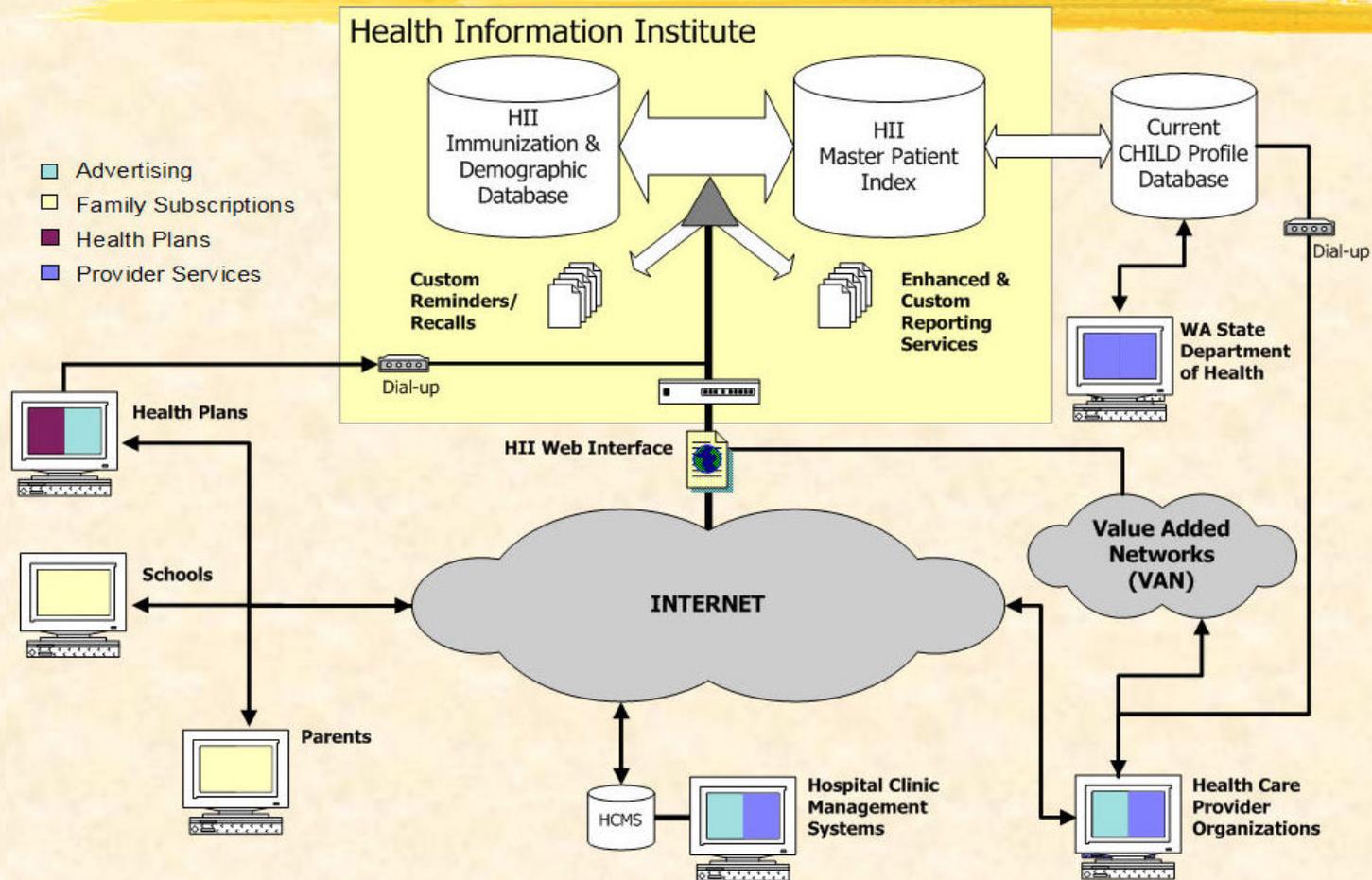


- Privately owned and funded database system
- Longitudinal immunization histories
- Internet accessible via secure channels
- Database retained and operated in secure environment

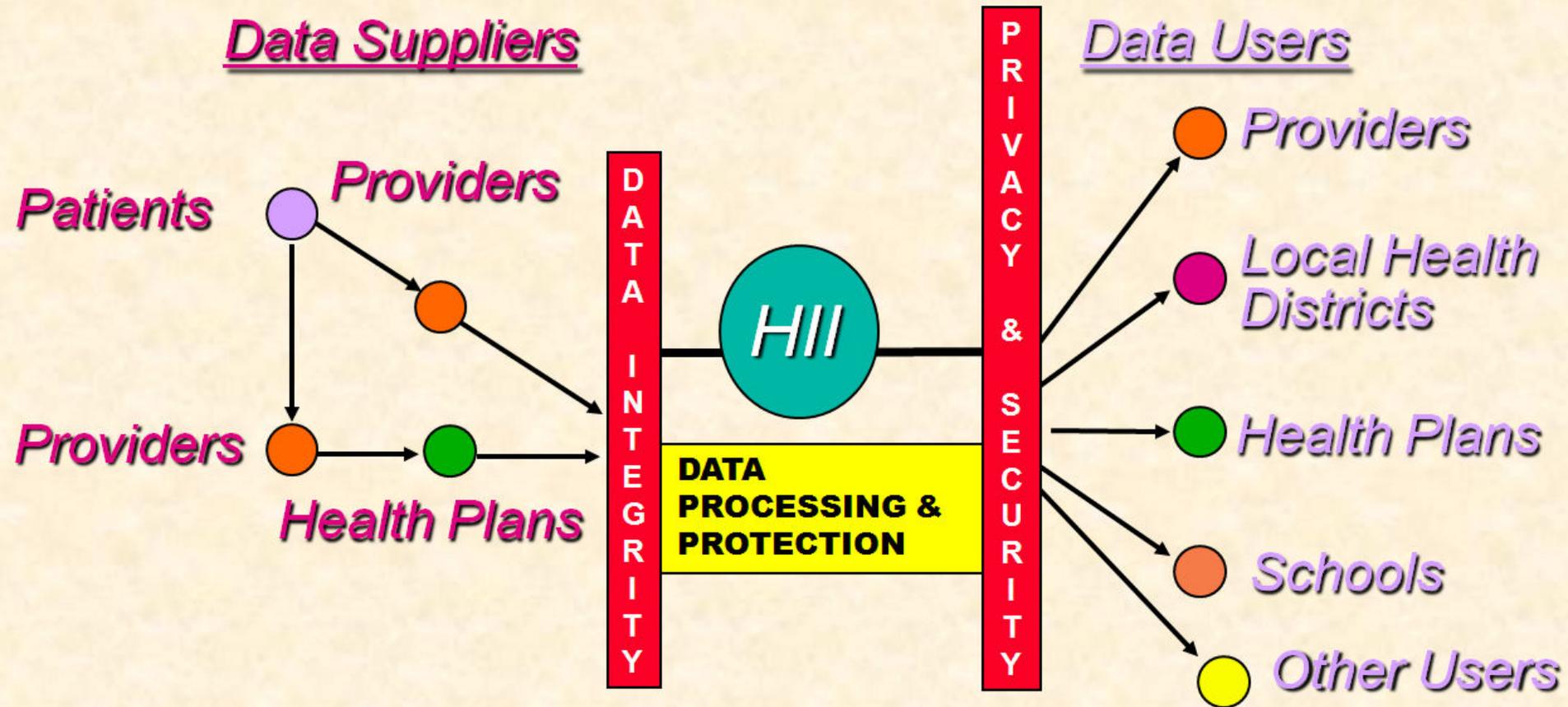
Information Flows



System Architecture



Legal Architecture



The Electronic Immunization Record



- *Multiple sources*
- *Reliable*
- *Accurate*
- *Complete*

Defining an Adequate Record



- *The Record Must Be:*
 - A reliable basis for patient care.
 - Confidential between physician and patient, and private as to third parties.
 - Admissible as evidence in court.

Defining an Adequate Record



- *A Reliable Basis for Patient Care Is:*
 - Based on physician/nurse observation and patient presentation.
 - Non-repudiable, accurate and complete.
 - Available when needed.

A Non-Repudiable Record



- *A Non-repudiable Record Is Created By:*

- Data sources bound by contract or policy
- Data from authenticated sources
- Careful classification of data
- A high integrity system platform

Contract or Policy Provisions



- Users accept obligation to provide only true, accurate and complete information and advise of potential errors.
- Users acknowledge that information will be relied upon by other providers, etc.
- System operator has the right to “police” reliability.

Data Source and User Authentication



- *Electronic Signatures: Verifying Who Sent the Message*
- *Authentication: Verifying the Message Has Not Been Altered*

Authentication by Public Key Authority

- *Certification Authority: Certifies that (a) Digital Signatures Come from the Correct Party and/or (b) Contents of Electronic Documents are Unchanged.*
 - Subscribers to Certification Authority Generate "Private Keys" and "Public Keys."
 - "Key:" Digital Code Sequence Subject to Mathematical Transformation.

Authentication by Public Key Authority



- *Hashing = Mathematical Transformation of Electronic Document Into Unique “Hash Result.”*
 - NOTE: Hashing is Applied to Digital Signatures Too.

An Accurate Record



- *An Accurate Record Is Created By:*
 - System design that let users easily classify and key in data for processes, procedures and outcomes
 - Well trained users
 - Acknowledged user entitlement to rely on data provided

Record Completeness



- *A Complete Record Exists When:*
 - All events, processes and outcomes recorded
 - Evidence of source of data immediately available
 - Rigorous editing and performance audits

Legal Use of Electronic Record

- *Admissibility in Evidence as the Ultimate Legal Test of Record.*
- *Requirements for Admission:*
 - Circumstantial guarantees of trustworthiness.
 - Evidence showing that the system produces an accurate result.

Clinical Use of Electronic Record

- *Acceptance by Users as Ultimate Operational Test of Record*
- *Requirements for Acceptance by Users*
 - Confidence in the technology and database manager
 - Right to rely on data sources
 - Readily accessible and easily understood interface

Protecting Electronic Medical Records

- *Confidentiality Binds Providers Not to Disclose Without Patient Consent or Privilege.*
- *Privacy Limits Third Party Rights to Obtain, Use or Disclose Individually Identifiable Health Care Information Without the Individual's Consent*

Protecting Electronic Medical Records



- *Security is the Set of Measures Adopted to Protect Information and Systems, Including Data Confidentiality, Integrity and Availability.*

System Security Architecture Elements



- *Intelligent System Design: Single best technological security control. Servers, terminals, communication links established in secure settings; network limited in scope and openness, etc.*

System Security Architecture Elements

- *Firewalls: Screen and limit access from external sources into internal network.*
- *Encryption: Converts legible information into code readable only by application of key which is retained by sender and receiver.*
- *Authentication: Devices, including passwords and digital signatures, to ensure identity of authorized users.*

Legal Security Architecture Elements



- *System Operator Obligation to Ensure System Security.*
- *User Obligations to Ensure Site Security.*
- *Identification and Limitation of Personnel Entitled to Access*
- *Provisions for Mandatory Increases in Security Measures and Privacy Procedures to Meet Evolving Standards.*

Legal Security Architecture Elements



- *No Use or Disclosure By Any Party Without Written Patient Authorization Except for Privileged Care Uses.*
- *Mutual Audit and Termination Provisions for Breach*
- *Mutual Indemnification Provisions*
- *Provisions for Mandatory Increases in Security Measures to Meet Evolving Standards.*