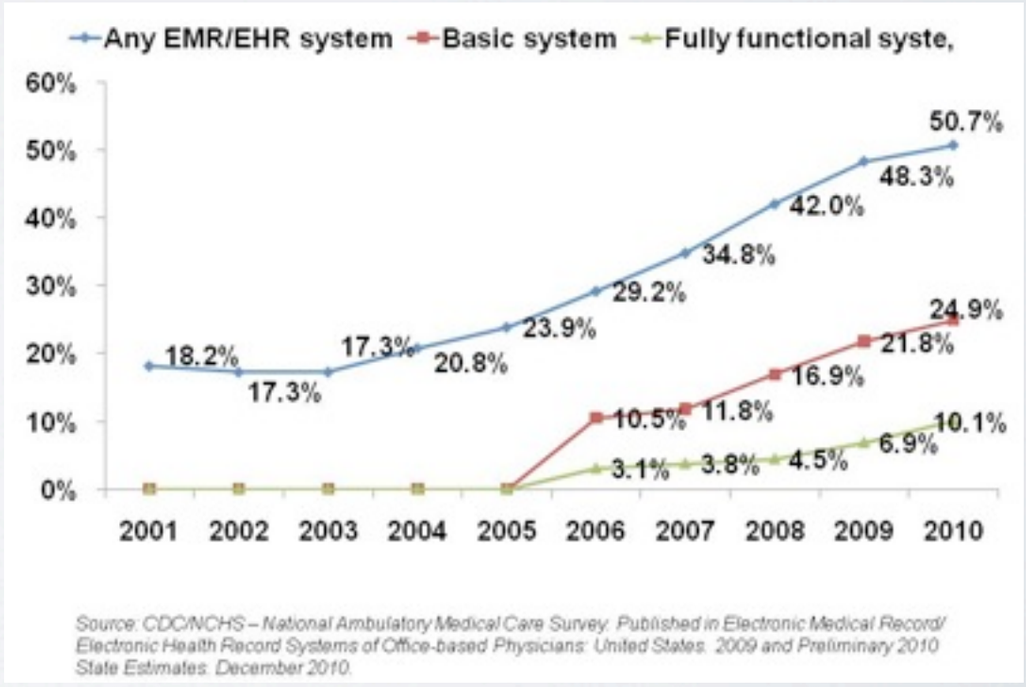
A Research Roadmap for Healthcare IT Security inspired by the PCAST Health Information Technology Report

Matthew Green and Avi Rubin
Johns Hopkins University

Background

- Increasing deployment of Electronic Health Records (EHRs)
  - Largely driven by legislation
  - Highly vendor-specific
- Data security is at a very early stage
- Many open questions regarding data sharing



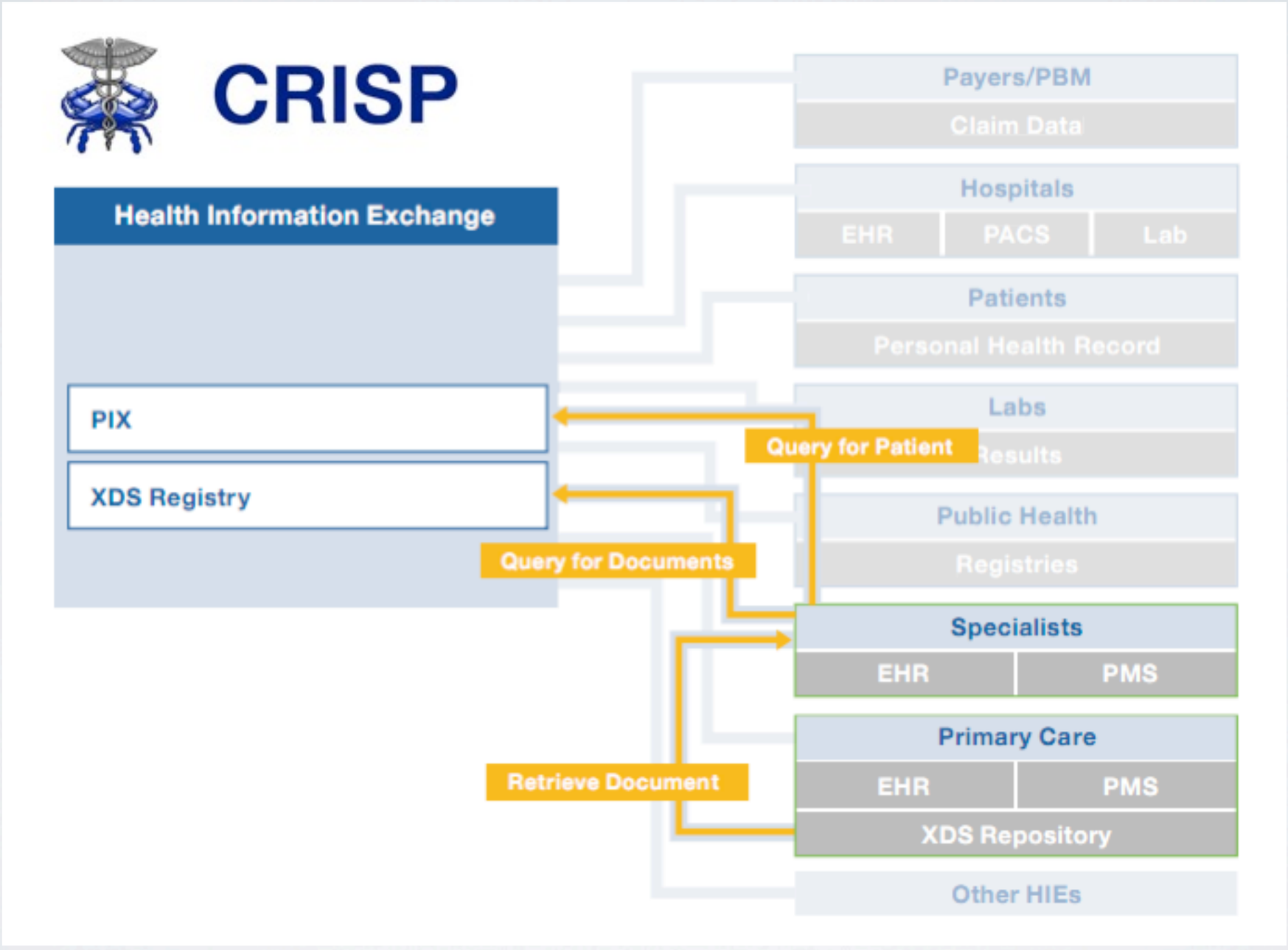
Source: CDC/NCHS – National Ambulatory Medical Care Survey. Published in Electronic Medical Record/ Electronic Health Record Systems of Office-based Physicians: United States, 2009 and Preliminary 2010 State Estimates: December 2010.

Background: Legislation/Standards

- HIPAA
  - Complex legislation
  - Primarily focused on procedures and policies
- HITECH Act
  - Intended to promote the use of EHRs via mandates and incentives
  - "Meaningful use"
- CCR/CCD
  - "Self-protecting" records (but how?)

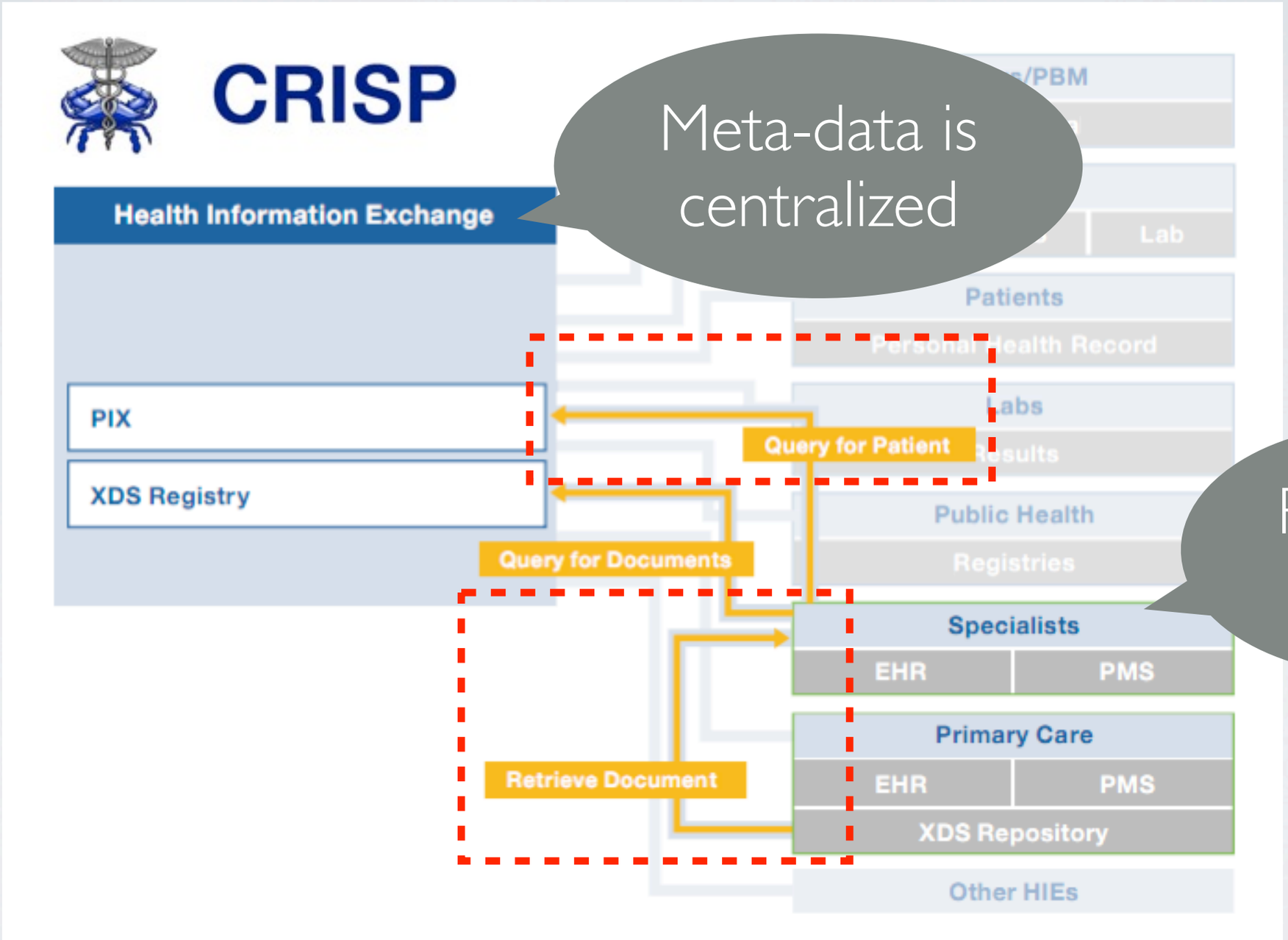
EHR Sharing: Existing Approach

EHR Sharing: an HIE Example



Locating and Retrieving Records in the CRISP Health Information Exchange

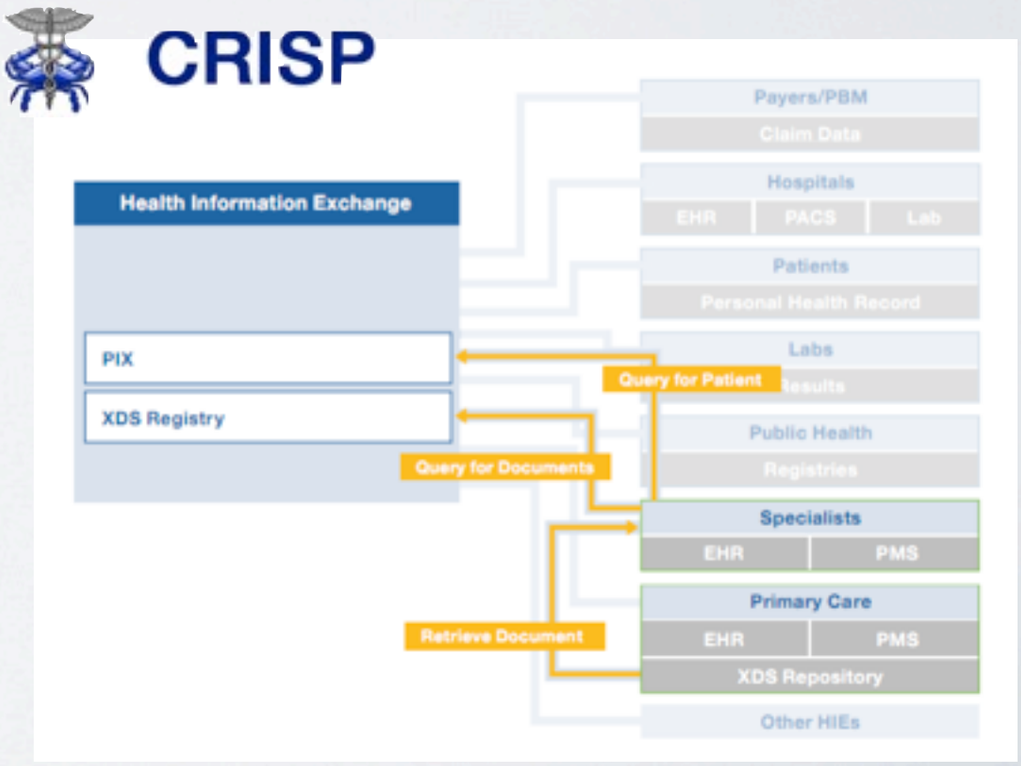
EHR Sharing: an HIE Example



Locating and Retrieving Records in the CRISP Health Information Exchange

EHR Sharing: an HIE Example

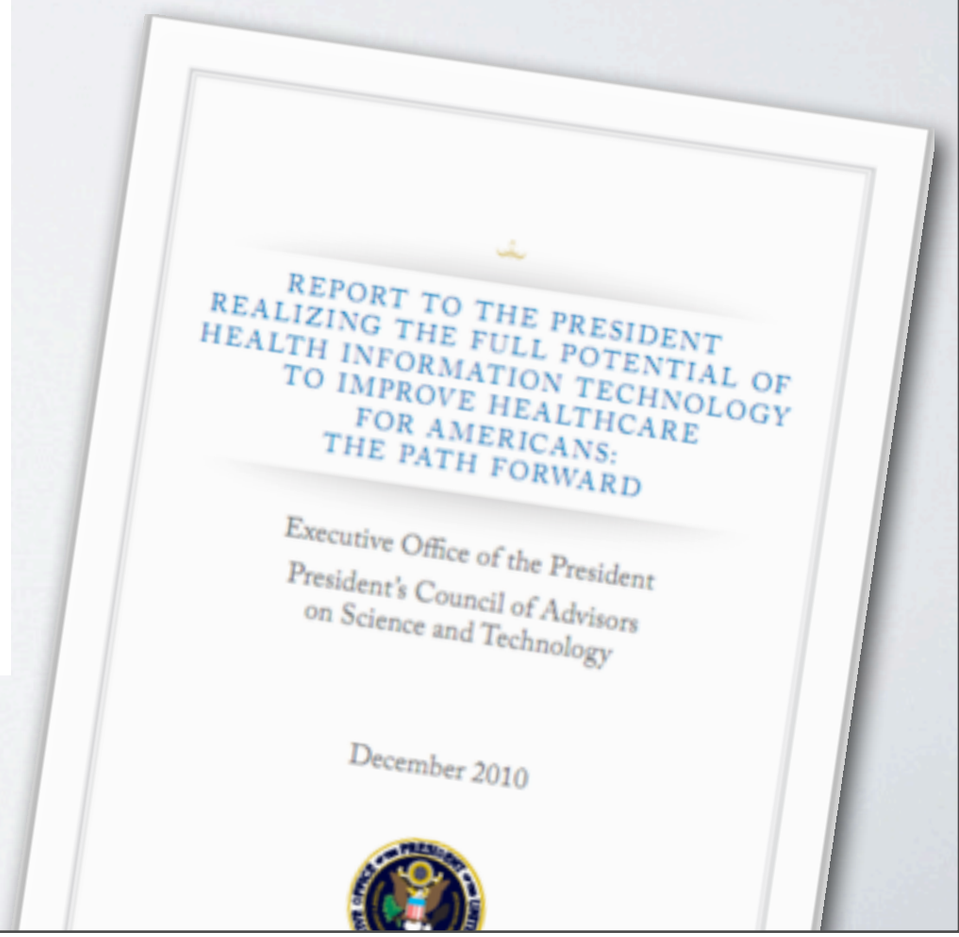
- HIE security reasoning (CRISP/Axolotl)
  - Data records should never leave hospital-owned machines
  - But in practice, "hospital" includes edge devices at the HIE data center
- Security and access control therefore depend on the integrity of each hospital's (large, distributed) Trusted base



The PCAST Report

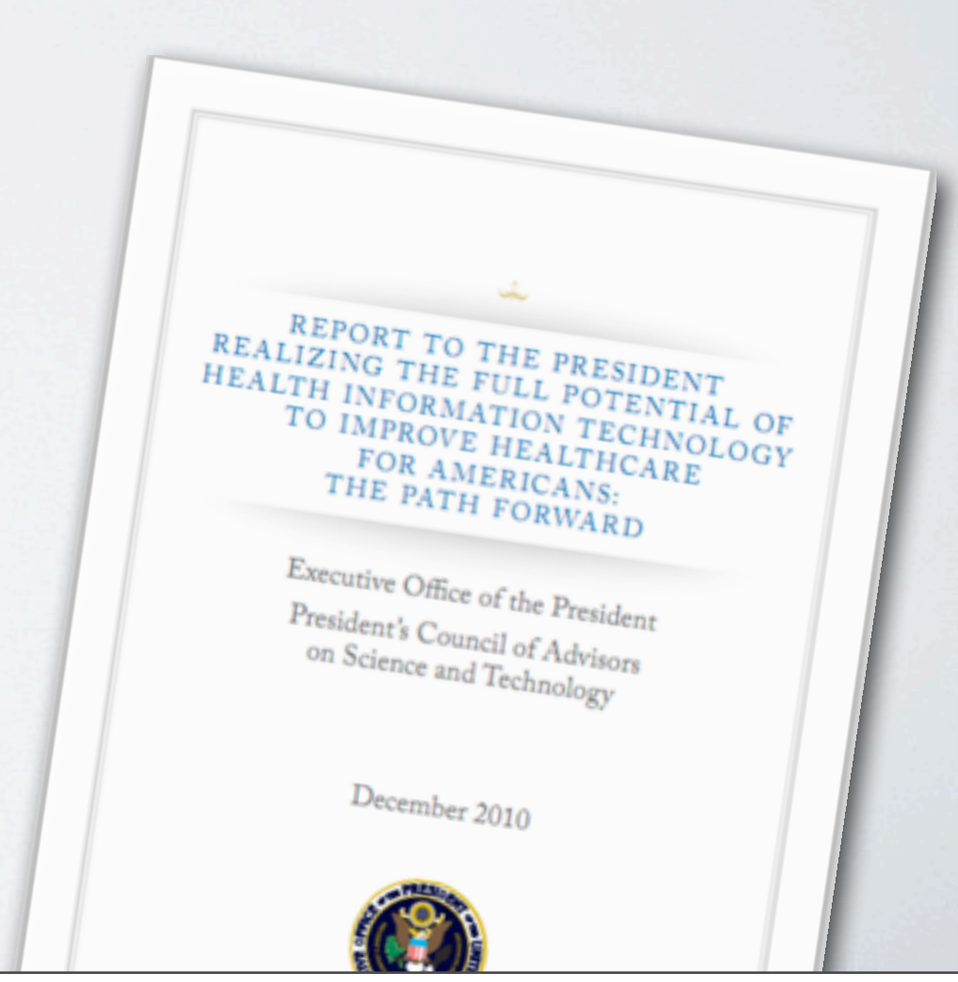
- President's Council of Advisors on Science and Technology
  - "Realizing the Full Potential of Health IT"
  - Security & need for data sharing are key points:

> *"American ambivalence about integrating health IT into the healthcare system is rooted in significant part to concerns about privacy and security."*
>
> *-Chapter V*



The PCAST Report

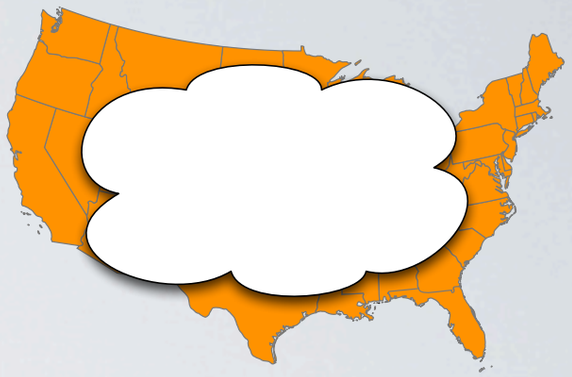
- President's Council of Advisors on Science and Technology
  - Solution: proposal for nationwide HIE
    - Use "meta-tagging" for record discovery, security policy
    - Cryptographic access control
- Good ideas, but only as good as their *implementation*
  - A great deal of work still needs to be done


REPORT TO THE PRESIDENT
REALIZING THE FULL POTENTIAL OF
HEALTH INFORMATION TECHNOLOGY
TO IMPROVE HEALTHCARE
FOR AMERICANS:
THE PATH FORWARD

Executive Office of the President
President's Council of Advisors
on Science and Technology

December 2010

PCAST Security Proposal



- Principles for a nationwide HIE
  - Data must be widely shared and discoverable
  - Data needs to self-protect via cryptography
    - *Data sharing organizations will not all be trustworthy*
    - Separation of the key & data planes
- Policies and meta-data must be standardized
- Patients need control over their security policies
- It must all scale!

User's Local System

(1) User authenticates him/ herself to the local system, within the context of an authorized role

(1)

(9)

(10)

Local Server

(9) Local server decrypts data elements and makes available to user

(10) After use, system destroys cleartext and key, possibly retaining ciphertext

(5) Local server requests data from locators returned from DEAS

(5)

(6)

(6) Data storage location server mediates request and returns encrypted records to local server

Data elements encrypted, with keys stored in DEAS Key Management Service

Data Storage Location

(7) On behalf of authenticated and authorized user and role, server sends DEAS request for encryption key for each data element provided

(7)

(2)

(9)

(4)

(2) On behalf of authenticated and authorized user and role, local server sends metadata search parameters to DEAS

(4) DEAS returns data locator list (e.g., URIs) resulting from metadata search

(9) DEAS returns key to local server, along with digitally signed privacy preferences

DEAS Services Bus

(3)

DEAS Security Mediation and Audit Services

Query mediation, transaction auditing, real-time audit analysis

(3) DEAS mediates request and searches metadata as permitted by privacy metadata within context of authorized role sent with query; transaction is recorded in audit trail

(3)

DEAS Metadata Search Service

Metadata indexed and tagged in accordance with individual consumers' consents

(8)

(8) DEAS mediates request, and retrieves key as authorized from key management service; transaction is recorded in audit trail

(8)

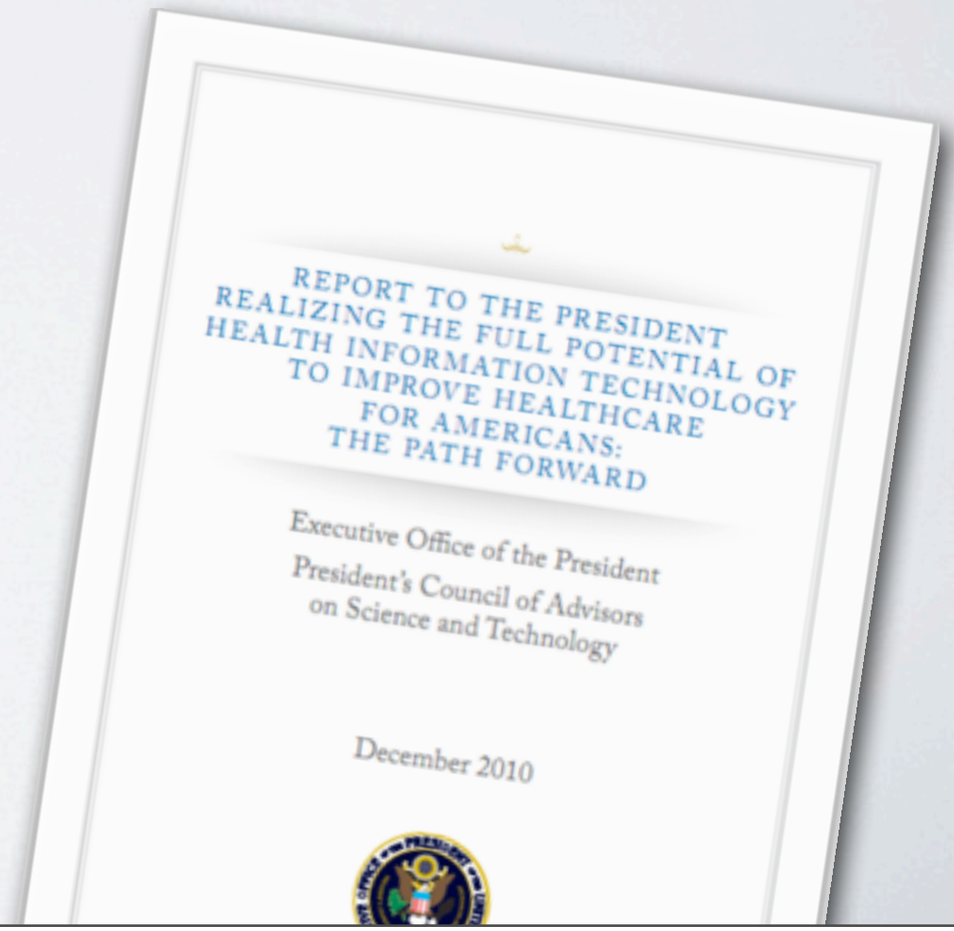
DEAS Key Management Service

Decryption keys stored apart from metadata and clinical data

Data Element Access Services (DEAS)

This talk is full of questions

- Where does this leave the research community:
    - What areas do we already understand?
    - What areas do we need to understand?
    - Will this system work?
    - How do we measure it?



Open Research Areas

- Meta-tagging
- Robust User Identity
- Audit and Logging
- Patient Access
- Cryptographic Key Management
- Dispute Resolution
- De-identification for research
- Comparison to security of paper records

Meta-tagging

- PCAST Proposal:
  - Tag data with attributes & security policies (abstract)
- Research problems:
  - Need for a standardized tagging scheme
  - Policy engines for programmatic data tagging
  - Evaluating the privacy implications of meta-tag data
  - Distributed search capabilities

Managing User Identity

- Always a fundamental security problem
  - 100s of thousands of clinicians (w/ roles), 100s of millions of patients!
- Research problems:

- Techniques for managing user identity from e.g., biometrics and other credentials
- New authentication techniques that are not dependent on a single, trusted party (e.g., RSA, Verisign)

Audit & Logging

- PCAST proposes:
  - Record the principal & authorization method associated with every EHR modification
  - Patients have the right to view logs
- Research problems:
  - New techniques for logging in a distributed environment
  - Log techniques that interact with a medical environment and can be examined by patients
  - Tamper-resistant logging

Patient Interaction

- PCAST proposes:
  - Users must interact with their own medical record, and specify policy
- Research problems:
  - Develop user friendly mechanisms for dealing with the complexity of user-selected privacy preferences.
  - Research how much data to make available to patients and in what format, different access to different patients based on certain criteria.
  - How to enable patients to delegate their access rights

Cryptographic Access Control

- PCAST proposes:
  - Records should be protected *cryptographically*, separating key and data plane.
  - Decryption only occurs in clinician computers.
- Research problems:
  - New techniques: e.g., policy-carrying cryptographic constructions (functional encryption, ABE)
  - Key management solutions, trusted hardware
  - Cryptographic mechanisms to *anonymize* records as required by secondary use considerations

Dispute Resolution

- PCAST proposes:
  - Users should monitor their own records and dispute invalid information

- Research problems:
  - Interface for securely monitoring patient health records.
  - Mechanisms for patients to dispute details of the EMRs, while preserving the original record.
  - Develop automated conflict resolution techniques (when a patient's claim about their EMRs differ from those of a health care provider such as a doctor or a laboratory.)

De-identification for Research

- PCAST suggests:
  - The availability of this (searchable) data will be a boon for medical researchers
- Research problems:
  - Analysis of de-identification techniques (and re-identification)
  - Aggregation and on-the-fly determination of privacy leakage, e.g., Dwork's Differential Privacy

Security Metrics

- PCAST Suggestion:
  - Develop metrics to evaluate EHR security
  - Use paper records as a baseline
    - How does this work in a data sharing environment?
  - Can we construct something more sophisticated that applies to existing HIE approaches as well?

Other Research Areas

- Implantable devices
- Home monitoring technologies
- Formal methods research (e.g., meta-tags)
- Legal issues
- Social science studies (user interaction)

Conclusions

- PCAST (or something like it) will happen
  - It can happen with, or without researchers' input
  - It serves as an excellent frame for any research efforts involving EHRs or sensitive medical information
- There's a great deal of work to be done