It’s a Jungle Out There! Protecting Consumers’ Privacy and Safety in an eHealth World

Dixie B. Baker, Ph.D.
Senior Vice President and Chief Technology Officer, Health Solutions

August 27, 2009

SAIC
From Science to Solutions

09-2217

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) – Fast Forward

- Today, only about 75% of reimbursement claims are submitted electronically – other administrative standards are used less than 50% of the time
  - Approximately $30B per year could be saved if all administrative transactions were electronic!
- Electronic Health Records (EHRs) have been adopted by many large health systems and are now beginning to penetrate into private practices
- Health Information Exchanges (HIEs) are springing up throughout the country, facilitating EHR sharing, e-prescribing, public health surveillance, and other shared services
- Personal Health Records (PHRs – e.g., Google Health, Microsoft HealthVault) and health record banks have emerged – until now, completely outside the reach of HIPAA

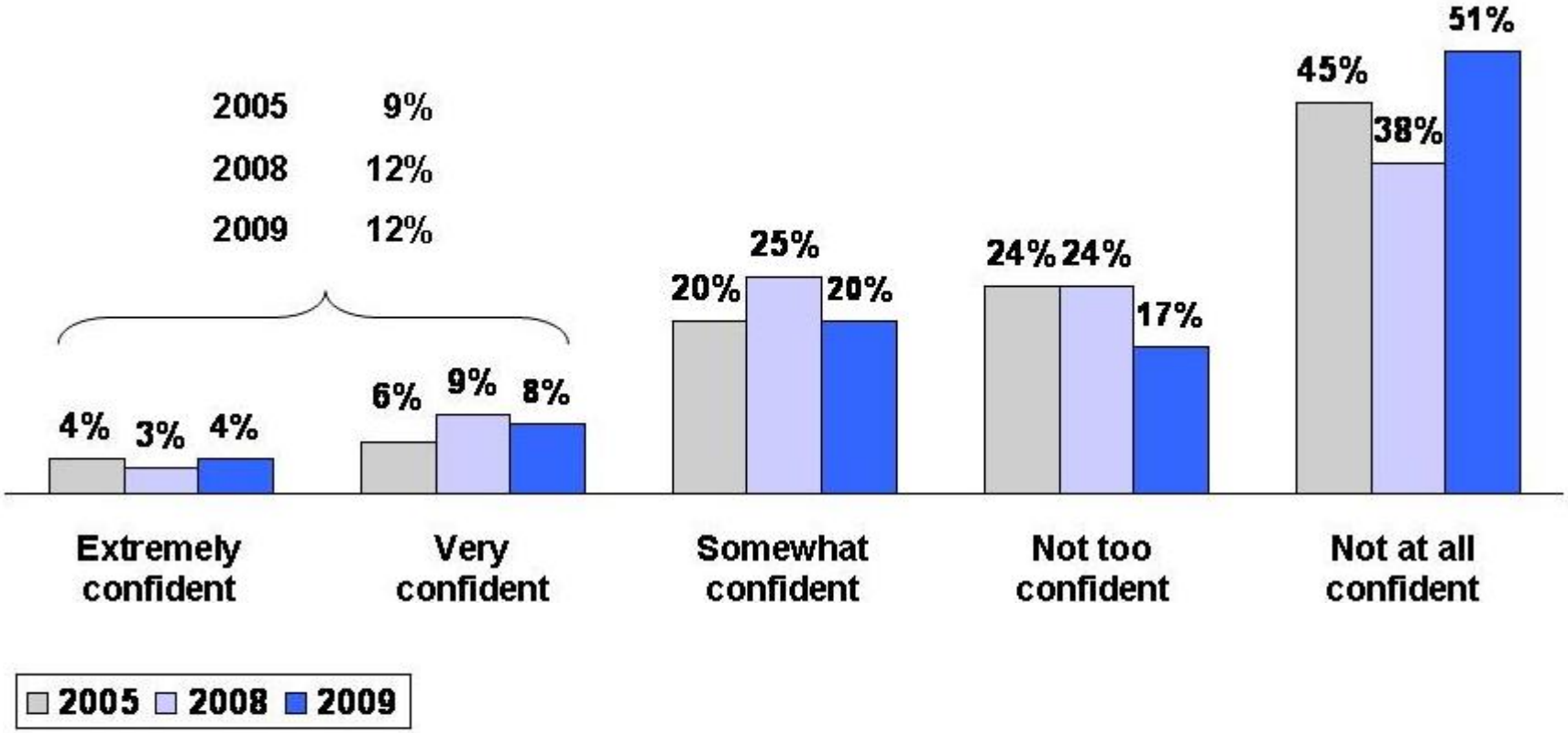
© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

HIPAA – Fast Forward (cont.)

- Security risks are ubiquitous, and increasingly nefarious
  - Virtually everyone is targeted by spyware on a daily basis, and many have been victimized by identity theft
  - Both techno-savvy and not-so-savvy consumers now recognize that the use of computers introduces new risks to their health information and their personal privacy
- U.S. has experienced terrorist and bioterrorist attacks, and natural disasters requiring rapid medical containment and response
- Virtually no one has been penalized for HIPAA violations

Today's Consumers Have Little Confidence that Electronic Health Records Will Remain Confidential

If medical records and personal health information were to be stored electronically and shared through the Internet, how confident are you that those records and information would remain confidential? (2009 n=1,000)



Source: Employee Benefit Research Institute and Mathew Greenwald & Associates, 2008-2009 Health Confidence Survey

ARRA Privacy and Security Provisions

- The American Recovery and Reinvestment Act ("ARRA") acknowledged these risks by enacting new provisions that significantly strengthen Health Insurance Portability and Accountability Act (HIPAA) privacy and security protections
  - Broader scope of applicability for the HIPAA Privacy and Security Rules to encompass Business Associates
  - Transparency for breach victims
  - Tighter restrictions on use and disclosure of protected health information (PHI)
  - Stronger consumers' privacy rights
  - Stronger enforcement and sanctions

- In addition, ARRA included a scheme for stimulating the adoption of EHRs – with provisions for assuring privacy and security in both EHR products and in their "meaningful use"

ARRA Privacy and Security Provisions

- Business Associates (including Health Information Exchanges)
  - Must implement the same HIPAA administrative, physical, and technical security controls, and are subject to the same penalties, as covered entities
- Breach Transparency
  - Covered entities (CEs) must promptly (within 60 days) notify individuals whose health information may have been disclosed as a result of a security breach
    - If more than 500 people are affected, must notify the media and the Department of Health and Human Services (HHS)
  - Business Associates must notify CEs
  - Similar requirements for Personal Health Record (PHR) vendors, with reporting to the Federal Trade Commission (FTC)
  - Interim Final Rules for both HHS and FTC published 8/19/09

ARRA Privacy and Security Provisions (cont.)

- Tighter Restrictions
  - Covered entities may not receive payment for PHI without the individual's authorization, except for limited purposes such as public health, treatment or research
    - Payment for research disclosures may not exceed the cost of preparing and transmitting the data
  - Marketing exceptions are no longer permitted without individual's authorization if the CE receives payment from another party
  - CEs must use or disclose the "minimum necessary" or a "limited data set"

ARRA Privacy and Security Provisions (cont.)

- Privacy Rights
  - If patient requests that information not be shared with health plan, and pays full bill, CE must honor request
  - CEs that maintain EHRs must provide copies in electronic form, and at individual's request, must transmit copies to named third parties
  - CEs that maintain EHRs must, at an individual's request, provide an accounting of all PHI disclosures from that system, *including for treatment, payment and healthcare operations (TPO),* during the prior three years
  - Fundraising materials must provide a "clear and conspicuous" opportunity to opt-out, and choice to opt-out must be treated as a "revocation of authorization"

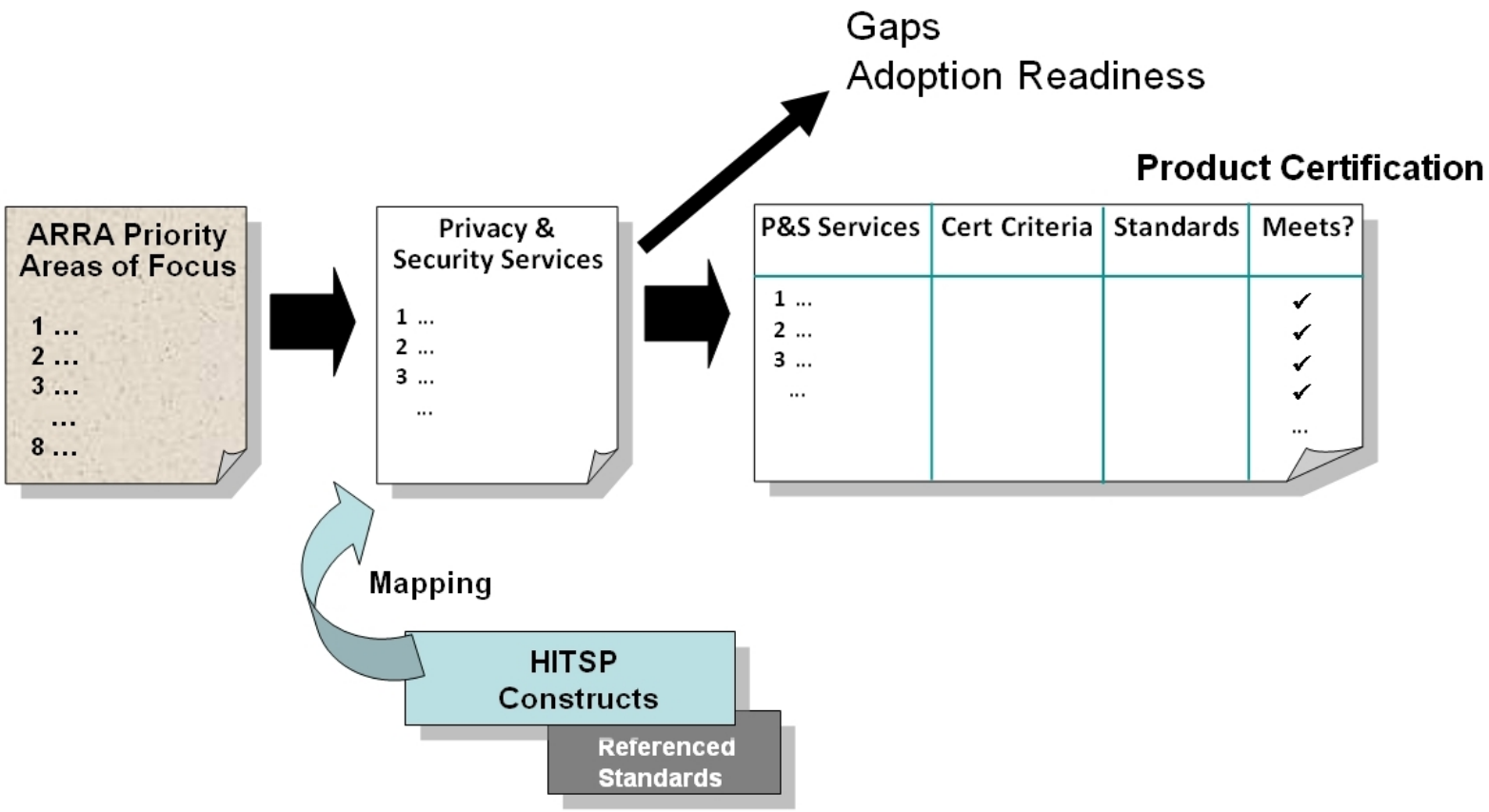
ARRA Privacy and Security Provisions (cont.)

- Stronger Enforcement
  - Any person who obtains PHI without authorization may be prosecuted
  - Incorporates notion of “willful neglect” – for which HHS must impose a penalty
  - New tiered civil penalties that consider degree of knowledge and culpability
  - State Attorneys General may bring civil actions on behalf of residents damaged by HIPAA violations
  - HHS Secretary must perform periodic compliance audits

Privacy and Security in EHR Adoption & Reimbursement

- To encourage broad adoption of EHRs, ARRA offers reimbursement to eligible providers who meet two requirements:
  1. Acquire a certified EHR product or service
  2. Demonstrate that the product/service is being used "meaningfully"
- ARRA assigns to new HIT Policy and Standards Committees responsibility for recommending standards, implementation specifications, and certification criteria needed for the electronic exchange and use of health information, starting with eight priority areas
- Certification that a defined security or privacy function or service has been implemented in a product is not sufficient to demonstrate "meaningful use" (or even "use") of that function or service
- The HIT Standards Committee Privacy and Security Workgroup adopted an approach that addresses both the certification of products and the demonstration that a user is using the certified product "meaningfully"

Mapping "ARRA 8" to Product Certification Criteria



Eight ARRA Priority Areas – Mapped to Privacy & Security Functions

1. Technologies that protect the privacy of health information and promote security in a qualified electronic health record, including for the segmentation and protection from disclosure of specific and sensitive individually identifiable health information
2. A nationwide health information technology infrastructure that allows for the electronic use and accurate exchange of health information
3. The utilization of a certified electronic health record for each person in the United States by 2014
4. Technologies that as a part of a qualified electronic health record allow for an accounting of disclosures made by a covered entity
5. The use of certified electronic health records to improve the quality of health care
6. Technologies that allow individually identifiable health information to be rendered unusable, unreadable, or indecipherable to unauthorized individuals
7. The use of electronic systems to ensure the comprehensive collection of patient demographic data, including at a minimum, race, ethnicity, primary language, and gender information
8. Technologies that address the needs of children and other vulnerable populations

Example – Certification Standards Recommended

Source References

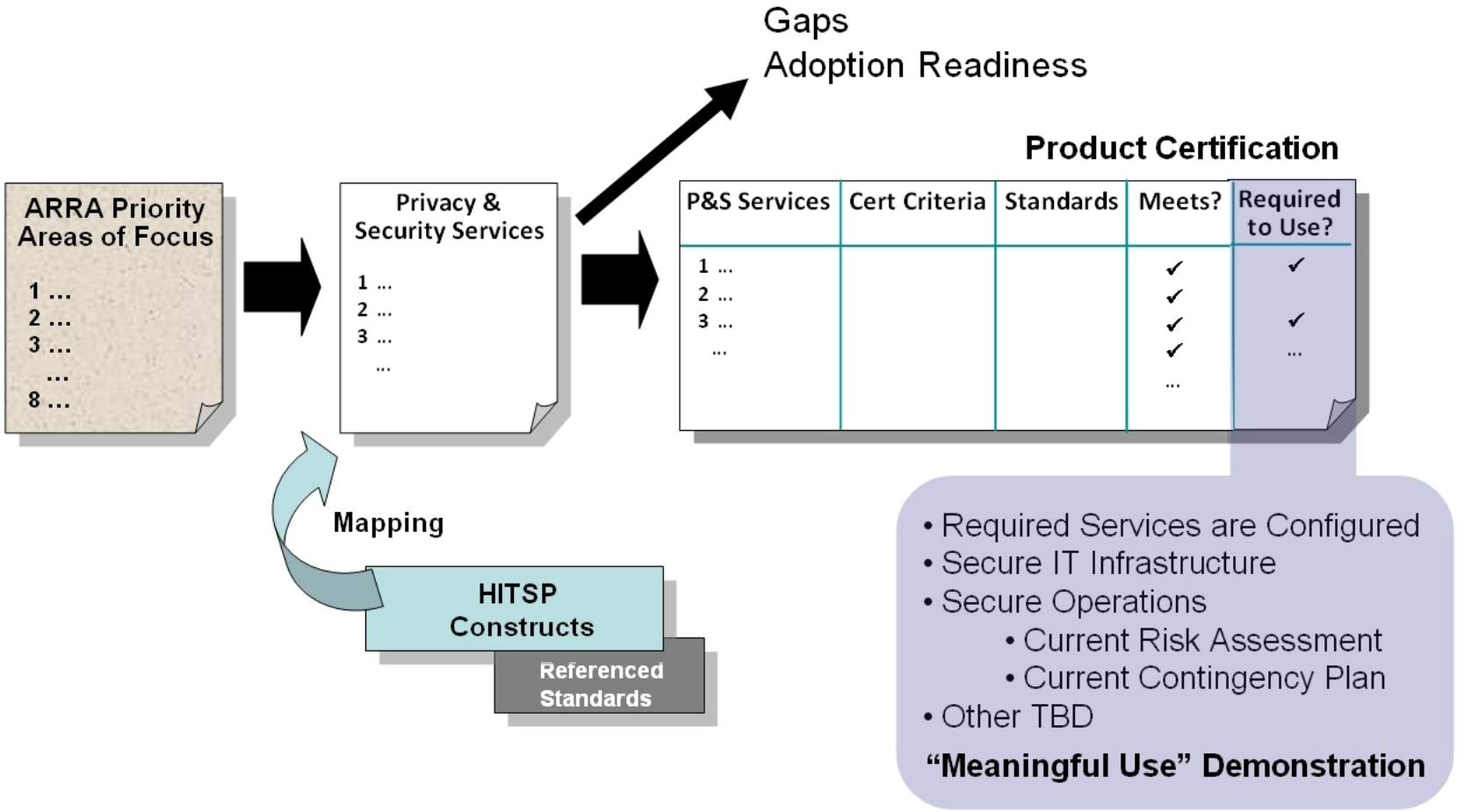
Services Supported

Implementation Timeline

Source Refs/ Cross-Refs	Short Title	Services Supported	Recommended Implementation Timeframe		
			2011	2013	2015
HITSP TP20/SC108	HL7 V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008	Access control		x	
HITSP TP20/SC108	OASIS eXtensible Access Control Markup Language (XACML), ITU-T Recommendation X.1142, February 2005	Access control			x
HITSP C19/TP20/ SC108	OASIS Security Assertion Markup Language (SAML) v2.0 OASIS Standard, ITU-T X.1141	Access control		x	
HITSP TP20/SC108	OASIS WS-Trust Version 1.3, March 2007	Access control		x	
HITSP T15/T17/ SC109	IHE ITI-TF Revision 4.0 or later, Audit Trail and Node Authentication (ATNA) Integration Profile, Section 9.1 Authentication	Audit		x	
IHE EUA	IETF RFC 4120. The Kerberos Network Authentication Service (V5). July 2005	Authentication	x		
HITSP TP30	IHE ITI-TF Revision 5.0 Volume 2 Supplement 2007 – 2008 Cross-Enterprise Document Sharing-B (XDS.b)	Authentication; Consent Mgmt		x	

SAIC From Science to Solutions

Mapping "ARRA 8" to Meaningful Use Criteria



Challenges

- Only objective identified by the Policy Committee was “HIPAA compliance”
  - All applicants are required by law to operate in compliance with the HIPAA Privacy and Security Rules
  - Including ARRA provisions, eventually – for now, including ARRA measures
- Requiring applicants to “recertify” compliance with some HIPAA standards and/or implementation specifications may suggest that some HIPAA requirements are “more important than others”
- Must avoid prescribing “new law” or “new regulations”
- Recognition that meaningful use of EHR technology unquestionably brings new privacy and security risks to the provider organization and consumers
  - ➡ Effectively addressing these risks is critical to the ultimate objective of furthering the adoption and proliferation of interoperable EHRs and HIEs

HIT Policy Committee "Meaningful Use" Objectives and Policy Measures

Objectives	Policy Measures
• Compliance with HIPAA Privacy and Security Rules and state laws	• Full compliance with HIPAA Privacy and Security Rules • Conduct or update a security risk assessment and implement security updates as necessary • Recommend that CMS withhold meaningful use payment for any entity until any confirmed HIPAA privacy or security violation has been resolved

Privacy and Security "Meaningful Use" Measures Recommended

- Recommendations include:
  - Measures representing value that EHR adoption is contributing to an enterprise's HIPAA compliance
  - Measures representing changes in the enterprise's approach to HIPAA compliance, as a result of its having adopted an EHR
    - Countermeasures to new risks
    - Configuration of security and privacy capabilities inherent in the certified product
  - Measures that can be objectively assessed by HHS

“Meaningful Use” Recommended Measures

Policy Measure:

- *Full compliance with HIPAA Privacy and Security Rules*

Demonstration Measures:

- Update and implement security and privacy policies to specifically address use of the certified EHR product in its operational environment in compliance with HIPAA Privacy and Security Rules and guidelines, including ARRA provisions:
  - Notification of individuals whose PHI may have been breached
  - Limiting disclosures to minimum necessary or limited data sets
  - Providing an accounting of all disclosures
  - Enabling consumers to request and receive electronic copies of their EHR
- Configure EHR system and supporting IT infrastructure in compliance with HIPAA Privacy and Security Rules and guidelines (including ARRA)

“Meaningful Use” Recommended Measures

Policy Measure:

- *Conduct or update a security risk assessment and implement security updates as necessary*

- Demonstration Measures:
- Conduct or update security and privacy risk assessment, and implement policy, procedures, and system configuration necessary to use the certified EHR meaningfully, including:
  - Termination of system access of terminated workforce members
  - Establishment and periodic review of accesses to assure that access is granted to those with permission, and that access is not granted to those who do not have permission
  - Protection against, detection, and reporting of malicious software
  - Monitoring of audit trail of system activities
  - Password-management (if passwords are used for user authentication)

“Meaningful Use” Recommended Measures

Policy Measure:

- *Conduct or update a security risk assessment and implement security updates as necessary*

- Demonstration Measures:
- (risk management – continued)
  - Screen-locking and session termination after pre-established periods of inactivity
  - Secure hash function to protect the integrity of all PHI transmissions
  - Encryption of all PHI transmissions, internal or external to the organization, where the possibility of their going over unsecured wireless or cellular networks cannot be ruled out
  - Encryption of all PHI transmissions that leave the facility and travel in part over shared networks
  - Encryption of all PHI stored on portable devices and removable media

“Meaningful Use” Recommended Measures

Policy Measure:

- *Conduct or update a security risk assessment and implement security updates as necessary* (cont.)

Demonstration Measures:

- Update and implement Contingency Plan (data backup plan, disaster recovery plan, emergency-mode operations plan, testing and revision procedures, applications and data criticality analysis) that incorporates use of the EHR product
- Identify and document data and capabilities that are minimally required in order to assure continuity of critical data services, and establish service-level-agreements (SLAs) consistent with these priorities

“Meaningful Use” Recommended Measures

Policy Measure:

- *Recommend that CMS withhold meaningful use payment for any entity until any confirmed HIPAA privacy or security violation has been resolved*

Demonstration Measure:

- To the extent possible, obtain confirmation from the Office for Civil Rights (OCR) that any confirmed HIPAA privacy or security violations have been resolved
- Obtain an affirmation from the entity at issue that any confirmed HIPAA privacy or security violations have been resolved

Current Work

- Reformatting standards recommendations to incorporate “base” capabilities required by HIPAA Privacy and Security Rules, and ARRA; and to clarify where options exist
- Collaborating with Policy Committee to refine privacy and security policy and standards moving forward
- For complete listing of recommended standards:
  - http://healthit.hhs.gov/portal/server.pt

    > HIT Standards Committee > Meetings > Past Meetings - 8/20/2009
- For Breach Notification Interim Final Rule:
  - http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf