Health IT Privacy Briefing to the Information Security and Privacy Advisory Board

April 7, 2010

Federal Panelists

- **Ms. Gail Belles**
  - ***Veterans Health Administration (VHA), Office of Health Information;*** *Director, Health Care Security Requirements*
- **Mr. Adam Greene**
  - ***Health and Human Services, Office for Civil Rights****; Senior HIT and Privacy Specialist*
- **Ms. Joy Pritts**
  - ***Health and Human Services, Office of the National Coordinator****; Privacy Officer*
- **Mr. David McDaniel**
  - ***Veterans Health Administration (VHA), Office of Health Information;*** *Privacy Compliance Assurance Officer*

Gail Belles

Director, Health Care Security Requirements

Office of Health Information

Veterans Health Administration

Health Information Exchange (HIE) Goals

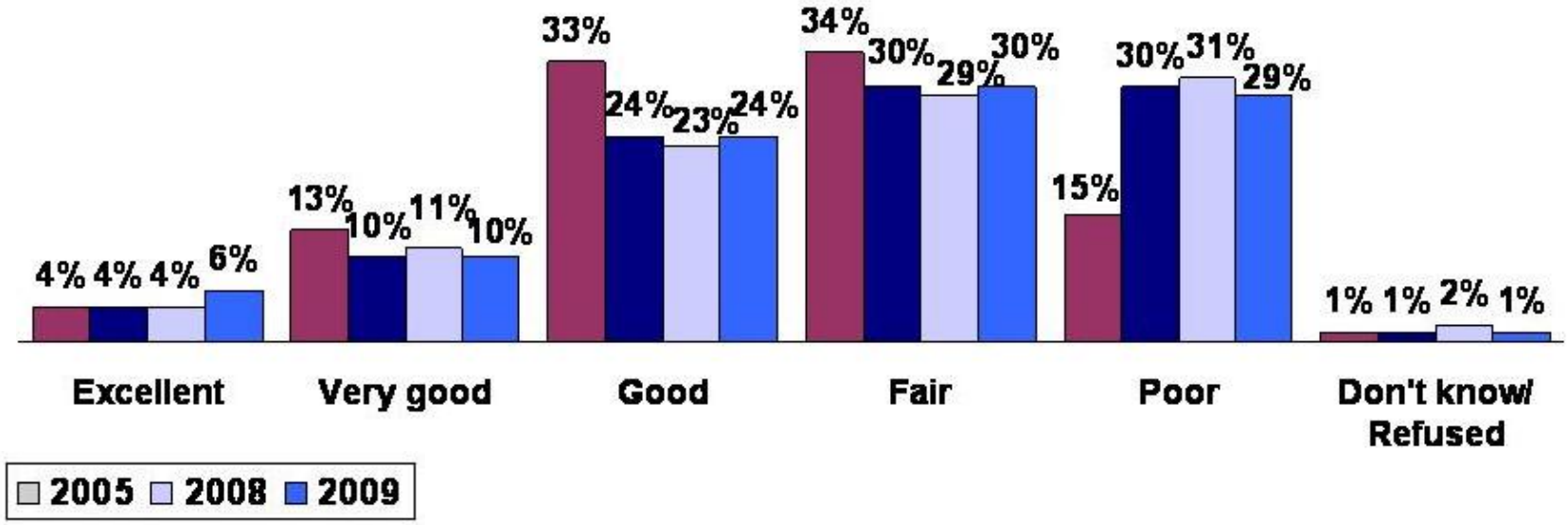
- Foster development of a “nationwide health IT infrastructure that allows for the electronic use and exchange of information”
- Enable secure information exchange between Federal and non-Federal entities to:
  - Improve health outcomes (measurement and comparison)
  - Advance patient-centered health care
  - Reduce errors and health disparities
  - Make health information available whenever and wherever it is needed
- Eliminate barriers to the exchange of health information across jurisdictions

Operational and Legal Issues

- Minimum Necessary
- Access to health information
- Opt in or opt out
- Variations in state law
- Notice of privacy practices
- Patient education
- HIE participation agreements

Consumers: 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

Federal Partner Panel Discussion

Perspectives of the Panelists in terms of Challenges and Current Approaches

- Adam Greene, HHS
- Joy Pritts, HHS
- David McDaniel, VHA

Adam Greene

Senior HIT and Privacy Specialist, Office for Civil Rights

Health and Human Services

HIPAA and eHIE

- HIPAA permits use and disclosure through HIE for:
  - Treatment
  - Payment
  - Health care operations
  - Pursuant to a HIPAA authorization
  - Pursuant to § 164.512 (e.g., public health, research)

Treatment

- Only health care providers conduct treatment
  - Requestor or discloser must be health care provider, or BA acting on provider's behalf
- Not subject to minimum necessary requirements
- Individual can request restriction
  - CE need not grant restriction

Payment

- Discloser can be health care provider or health plan
  - Or BA on either's behalf
  - CE may disclose for requestor's payment activities
- Subject to minimum necessary
- Individual can request restriction
  - CE need not grant restriction, except
  - CE must grant restriction on disclosing to health plan for payment or HCO if individual fully paid out-of-pocket

Health care operations

- CE may disclose for its own HCO
- CE may disclose for requestor CE's HCO if each CE has relationship with individual, and:
  - Limited to certain types of HCO (e.g., quality improvement, care coordination, reviewing practitioner qualifications); or
  - For health care fraud and abuse detection/compliance.
- Subject to minimum necessary
- Individual can request restriction
  - CE need not grant restriction, except
  - CE must grant restriction on disclosing to health plan for payment or HCO if individual fully paid out-of-pocket

HIPAA and HIE

Authorization vs. Consent

- HIPAA permits use and disclosure pursuant to an *authorization*
  - Authorization must meet HIPAA content requirements (and more stringent state criteria)
- Where no authorization is required (e.g., treatment), HIPAA permits covered entity to obtain *consent*
  - Matter of CE discretion
  - No HIPAA content requirements
- HIE system may need to process both HIPAA authorizations and consents
- HIPAA permits use of electronic signature as permitted by ESIGN Act
- No accounting requirement for disclosure pursuant to authorization

HIPAA and eHIE

Section 164.512

- Required by law
  - E.g., mandatory federal or state reporting law
- Public health
  - E.g., CDC, FDA, state biosurveillance activity
- Health oversight
  - E.g., CMS, OIG
- Certain research
  - E.g., IRB approval of authorization waiver
- Specialized government functions
  - E.g, Between DoD and VA

Minimum necessary

- Governs uses and disclosures other than treatment, to the individual, pursuant to an authorization, to the Secretary, or as required by law.
- Governs uses, disclosures, and requests by covered entities.
- Policies and procedures required for routine disclosures.
- CE may rely, if reliance is reasonable, on requests of other CEs as being for minimum necessary information.
  - CE may not rely on requests of non-CE as minimum necessary, except certain requests from public officials and researchers.
- May not use, disclose, or request entire medical record unless specifically justified.

Joy Pritts

Privacy Officer, Office of the National Coordinator

Health and Human Services

State Laws Regulating Use & Disclosure of Health Information

- Health traditionally been within purview of the states.
- Large body of state law existed prior to HIPAA Privacy Rule.
- Often sector specific.
- Few have comprehensive frameworks like HIPAA Privacy Rule.
- Much state law remains in effect due to HIPAA's preemption framework.

State Law: Significant Areas of Interest

Disclosure Restrictions

- Often intended to address a contemporaneous public health issue:
  - Tuberculosis
  - HIV/AIDS
  - Substance abuse
- Promise confidentiality to encourage testing and treatment
  - Require patient consent to share information

State Law: Significant Areas of Interest

- Medical record requirements
  - Record retention laws
  - Content of record
  - Ability to modify record
- Patient Access Laws
  - Minors
- Acceptable means of transmitting prescriptions
- Delivery of clinical laboratory test result

State Laws: Interdependencies

Other legal standards may be tied to “health information” privacy laws

- Tort law (*e.g.*, record retention)
- Reproductive rights

Federal Approach to State Laws

- Congress consistently has not been inclined to fully preempt state law in this area.

- HITECH (2009)
  - Opportunity to address and declined to do so.

ONC State Law Resources

Health Information Security and Privacy Collaborative (HISPC)

50-State Surveys and Reports on

- Medical Records Access
- Clinical Laboratory Release Laws
- State Prescription Laws
- State Disclosure Laws

David McDaniel

Privacy Compliance Assurance Officer, Office of Health Information

Veterans Health Administration

Still Learning the Ropes

- If this was easy, we would have likely done it long ago
- It is a mix of technical capabilities and standardizations with legislative requirements
  - Must balance the capability for fluid exchange of data with an individual's rights regarding data about them
- Still exploring what we "don't know we don't know"
  - As we broaden the net, we learn new pieces of the puzzle
- Early efforts are critical to defining how data-sharing will be best accomplished in large-scale
  - Not only in the health care space, but in other business needs for data such as are needed by Veterans Benefits Administration, Social Security Administration, etc.

NHIN, VLER and all points forward

- With whom and for what greatly impacts privacy implications in data exchanges
  - Authorities to use and disclosure are typically based on these two factors
- NHIN is somewhat less complicated since partners are HIPAA Covered Entities
  - Built-in consideration of business needs for data
  - Corresponding authorities to use and disclose for health care purposes
- VLER expands to non-HIPAA organizations who will need to share data with HIPAA Covered Entities
  - Business needs that are beyond the health care purposes
- Innovations may bring new situations

Does a Free-Flow of Data compete with Privacy Rights?

- Right to a Notice of Privacy Practices
  - Significant changes to privacy practices could require submission of new notice
    - Depending on CE, could be very costly
  - *Privacy right could be compromised if notice does not accurately reflect business changes resulting from data exchanges with multiple partners*
- Right to Request Restriction
  - Technical solutions need capability to allow for restrictions
  - HITECH requires support to restriction requests under certain circumstances
  - *Privacy right could be compromised if restrictions are allowed by some partners and not adhered to by other partners with the consumer expectation that it applies to their data regardless of who is using or disclosing it*

Does a Free-Flow of Data compete with Privacy Rights?

- Right to Request an Accounting of Disclosures
  - Front-load of disclosures in order to begin sharing process with partners. Requires large numbers of accountings at once
  - Staffing for manual processes required during startup
  - *Privacy right could be compromised if transition to new partners is not managed so that all bulk disclosures are accounted for by the disclosing partner*
- Right to Access
  - This is likely to be handled by each CE separately, but individuals may request data access in various forms
  - *Individuals could perceive that they have to forfeit their privacy right if not allowed to access their data from multiple NHIN partners. This would require managing consumer expectations in the electronic exchange world*

Does a Free-Flow of Data compete with Privacy Rights?

- Right to Request Amendment
  - May require coordination between NHIN partners if a request goes to one partner and the information was created by another partner in the exchange group
  - *Consumers may feel caught in the middle of a "sorry, not my data" scenario and feel that their right to request amendment is overly complicated*
- Right to Request Confidential Communications
  - This is likely to be handled by each CE separately, but individuals may request confidential communations once, assuming it applies to all partners
  - *Individuals could perceive that they have to forfeit their right to confidential communications if not allowed to have multiple NHIN partners contact them by an agreed-upon method. This would require managing consumer expectations in the electronic exchange world*

Does a Free-Flow of Data compete with Privacy Rights?

- Right to File a Complaint
  - Typically outlined in a CE's Notice
  - May require collaboration in investigating complaints against multiple partners
  - May change how HHS-OCR works with Covered Entities on complaints
  - *Potential confusion on how to file complaints when multiple data-sharing partners may be involved in a privacy infraction*

Private and Public Sector Differences

- Privacy Act of 1974
  - Accounting for disclosures
- Freedom of Information Act
- National Archives and Records Administration requirements for Federal Records retention and disposition
- Agency Requirements such as Title 38 protections
- State Law applicability to Federal agencies
- Legal organizational structures

“When you have apples and oranges, you better be good at making fruit salad”

Privacy Act Requirements on Federal Agencies

- Limitations on the collection, use and dissemination of personally identifiable information about an individual
- Disclosure restrictions to third parties.
- Access and amendments rights of the individuals who are subjects of the files.
- Notification to the public of collections of information on them (forms and web sites), and record systems (Federal Register Privacy System Notice. Secret records on individuals cannot be maintained.

Privacy Act Requirements on Federal Agencies

- Maintenance requirements:
  - Is the information relevant and necessary?
  - Is the information accurate, timely, and complete?
  - Is the information from the subject?
  - Is there a notice addressing the purpose and use of the information?
  - Are safeguards in place to protect the integrity of the information

CASE STUDIES

Partner Assumptions

- Common treatment relationship with patient gives HIPAA authority to share for treatment
- Minimum Necessary – can assume data requests by other Covered Entities are the minimum needed
- Compatible capabilities to afford privacy rights to individuals (Notice, Business Associates, etc.)
- The information passed ensures confidentiality, data integrity and is readily available when needed and is relevant, timely and accurate

Case Study – San Diego

- Partnered with Kaiser Permanente and DoD
- Start small with a few patients (1,200+/-)
- Participant letter was sent to consumers including authorization form
  - Not confident that consumers understood what they were signing or what authorization meant even though they will given call-in numbers to ask questions
- Manual processes for authorizations and used existing authorization forms
- Utilized existing processes and software for accounting for disclosures, but had to enter in bulk

Case Study – Med Virginia

- Piloting with a much larger number of patients (73,000+/-)
- Manual processes for authorizations still being utilized but authorization form is considerably simplified
  - A HIPAA-compliant authorization would have required specific elements not required by Title 38, 7332, but since authorization was to satisfy Title 38, it could be streamlined
- Utilized existing processes and software for accounting for disclosures, but had to enter in bulk
- Introduction of the concept that participant's data from San Diego pilot could be included for Med Virginia where there was a common treatment relationship

Lessons Learned

- Get all stakeholders to the table early and involve them in each process (even if it was done before, it may be different the next time)
- Simplify as many internal processes as possible ahead of time
- Have processes to manage the pilot before exchanges begin
- Train pilot-site staff so they know what to expect
- Include steps to manage consumer expectations
  - Participant letter clear and concise

SOME NOTABLE CHALLENGES

Authorization vs. Consent

- HIPAA has distinct differences between Authorization and Consent
- These each have specific business responsibilities that are different from each other.
- NHIN technical specifications refer to the transactions handling authorization and consent as “consent” requirements
  - This creates a terminology disconnect between privacy experts and technical experts during implementation
  - Introduces potential confusion between data-sharing partners as more partners come on-line

Title 38 Requirements for Sensitive Data Classes

- Only applies to VA data
- Requires signed authorization from individual subject
- Allowable for disclosures between VA and DoD but not other NHIN partners
- VA's EHR does not have the capability to separate protected information from non-Title 38 protected data
- Creates a privacy requirement disparity between VA and other NHIN partners
- VA seeking legislative relief for treatment disclosures

Non-HIPAA-Covered Partners

- Legal requirements are different
  - HIPAA was written with specific types of organizations in mind
    - Health Plans
    - Health Care Clearinghouses
    - Health Care Providers who conduct electronic health care transactions
- Authorities to share information are different
  - e.g., DoD can share with VHA for HIPAA-covered purposes but only with VBA at time the subject separates from the military
  - With other federal partners, these differences will have to be fully explored and addressed

Adding Other Partners

- Authorizations may only apply to existing partners
  - May require new authorizations to be signed
  - Participants may not want information shared with new partners
- Restriction ability becomes critical in this situation
- State law differences may impact requirements for data sharing and use/disclosure by partners

Wrap Up

- Health information exchange has tremendous benefits
  - Improve health care quality
  - Reduce costs
  - Empower consumers
- But privacy concerns can stand in the way of acceptance and use of systems by consumers and providers

QUESTIONS