FOURTHOUGHTGROUP

NHII and EHR: Protecting Privacy and Security - Current Issues and Recommendations

HIPAA Summit X – April 8, 2005

Carol A. Karps

Workshop Purpose

- To provide participants with an understanding of the issues and potential barriers to protecting privacy and security in the NHII and EHR

- To provide participants with an understanding of the current ideas and recommendations to protect privacy and security in the NHII and EHR

- To discuss participant ideas as to how HIPAA Privacy and Security Rules should be integrated

Resources for Presentation

- Framework For Strategic Action, DHHS July 2004
- Recommendations from NHII Conference, July 2004
- DHHS ONCHIT RFI, November 2004
- EHealth Initiative ONCHIT RFI Collaborative Response, January 2005
- Health Privacy Project ONCHIT RFI Response
- Miscellaneous papers, reports 2004-5

NHII/EHR VISION

DHHS Vision: Framework for Strategic Action

- Interoperable electronic health records
- Consumer centric information that follows the consumer – EHR/PHR
- Enhanced decision support tools
- E-Prescribing
- Increased telemedicine
- Medical records protected from unauthorized access
- Cost effective, quality care

ISSUES

- DHHS maintains that EHRs have potential to provide an easier means of meeting HIPAA Privacy and Security standards
  - Baseline for enhanced security standards laid out in the Security Rule
- The VA and DoD have secure, web-based systems for their beneficiaries

ISSUES, con't

- National focus has overlooked need to build in privacy and security protections at the outset in both architecture infrastructure and policy - Health Privacy Project

- Survey released 2/23/05 (P&AB and Harris Interactive):
  - 70% concerned that PHI could be disclosed because of weak data security
  - 69% concerned that an EHR system could lead to more sharing of health information without patients' knowledge
  - 47% report that privacy risks outweigh benefits of EHR

ISSUES, cont'd

- EHR Questions to be resolved include:
  - Who controls the information - patient, provider?
  - Who can disclose the information – specific provider or entity?
  - Which individuals have access to the system?
  - Who agrees to patient's request for disclosure restrictions?

ISSUES, cont'd

- NHII Standardization issues to be resolved:
  - **Need for further standardization of data elements, values, event descriptions, and message formats**
  - **Wide use and acceptance of existing standards and rapid adoption of new standards is a must**
  - **Standards are a prerequisite for integration and reuse of historical data and data collected from multiple sites**

ISSUES, cont'd

- Standardization issues also include:
  - Technical and policy requirements to enable interoperability
  - Local, regional and national " common framework"
  - Privacy and security guidelines and policy clarifications
  - Standard enforcement policies

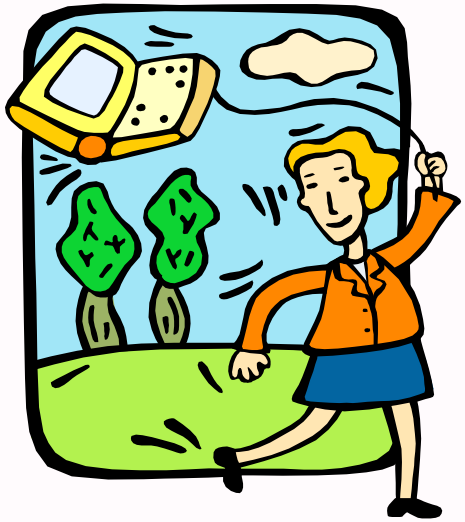
ISSUES, cont'd

- Other issues to be resolved include:
  - Health care entity participation – voluntary or mandated?
  - Financing and budget issues – startup, ongoing
  - Organizational Structures – state, local, regional networks?

BARRIERS

- "Buy-in" for NHII & EHR
  - Concerns that it would be a central data repository, ie "big brother"
  - Concerns of inadequate consumer involvement and protections
  - Concerns of a "big bang approach", rather than incremental
  - Provider concerns about liability
  - Disagreement on standards

BARRIERS, cont'd



- Involving, educating, and training consumers – who, how, when?
- Uneven enforcement and monitoring of HIPAA Privacy and Security Rules to ensure consumer protections
  - Complaint driven
  - Few enforcement resources

BARRIERS, cont'd

- Lack of technical specifications, standards and requirements essential for interoperability

- Lack of user friendly interface designs and implementation support

- Lack of standardization across covered entities in technical capacity and policies and procedures

BARRIERS, cont'd

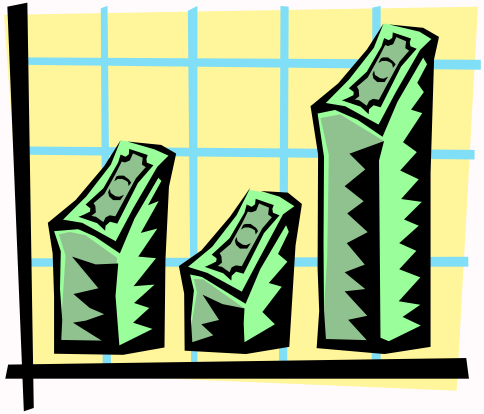
- Complexity, fragmentation, and volume of health care transactions

- Inconsistent payment policies and regulations with inconsistent reporting

- State HIPAA Privacy Preemption issues potential barrier to standardization, as well as inconsistency of laws for information sharing among states

BARRIERS, cont'd

- Health care entities already financially stressed due to HIPAA compliance and other pressures
- Inadequate capital for investment in technical infrastructure, systems, standards
- States have severe financial constraints and have been cutting health care funding and provider rates
- Federal matching monies limited to state Medicaid agencies



RECOMMENDATIONS

- NHII Conference, July 2004

  - **Analyze gaps in current privacy laws and develop policy that addresses use and disclosures**
  - **Cross industry group to create a Regional Health Information Infrastructure privacy model**
  - **Provide Federal leadership in resolving preemption issues**
  - **Interoperability body to develop and establish infrastructure to implement privacy and security mechanisms**

RECOMMENDATIONS, cont'd

- NHII Conference, July 2004
  - **Assign ownership of the EHR to the consumer**
  - **Ensure consumer involvement in standards development (local, regional, national advocates)**
  - **Ensure consumer support through**
    - ✓ **Strong security management**
    - ✓ **Clearly defined and enforced access restrictions**
    - ✓ **Extend Privacy and Security protections to telehealth, e-prescriptions, and email communications**
    - ✓ **Effective enforcement**
  - **Provide consumer education through community outreach and media**

RECOMMENDATIONS cont'd

- ONCHIT RFI – EHealth Initiative Response

  - **Establish a "common framework" consisting of technical and policy standards**
  - **Create a decentralized and federated model – Regional and sub-networks**
  - **Design to respect and serve patients/consumers**
  - **Uniform adoption of information sharing practices and enforcement sanctions within the model**
  - **Develop uniform policies for storage and retention of data**
  - **Establish financial sustainability models for the entity**

RECOMMENDATIONS, cont'd

- EHealth Initiative, cont'd
  - **Develop a regional/local Record Locator Service (RLS) that holds information authorized by patient**
  - **Develop network incrementally**
  - **Develop a national Standards and Policy Entity**
  - **Clarify privacy guidelines and policy re: HIPAA, anti-kickback, potentially conflicting state laws, and anti-trust laws**
  - **National enforcement policies for misuse of data**
  - **Develop performance and accountability metrics**
  - **Coordinated efforts to educate public**

RECOMMENDATIONS, cont'd

- ONCHIT RFI - Health Privacy Project

  - **Urge the development of a strong public education and participation effort**
  - **Build NHII based on connecting local and regional systems**
  - **NHII must be rooted in fundamental principles of privacy**
  - **NHII must adopt protections under HIPAA Privacy Rule and be flexible to incorporate more stringent state privacy laws**

RECOMMENDATIONS, cont'd

- Health Privacy Project, cont'd
  - **Participation in NHII must be voluntary for patients**
  - **Patients must have significant control over their personal health information**
  - **Strong enforcement regulations must ensure adherence to privacy and security laws and policies**
  - **Address privacy concerns of patients as foremost in efforts to improve technological health care infrastructure**

RECOMMENDATIONS, cont'd

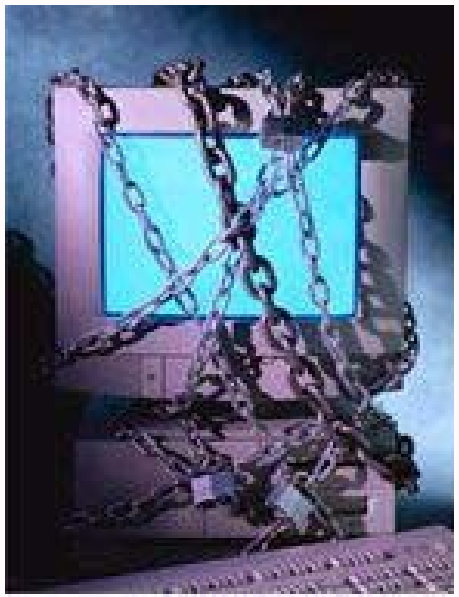
SUMMARY

- HIPAA could be a building block for NHII
- Rapid adoption and consensus for national standards and practices
- Increased enforcement of HIPAA Privacy and Security
- Clarify Privacy Preemption
- Ensure consumer involvement and protection

Integrating HIPAA Privacy and Security

Discussion Points

Does the move to all electronic health records, rather than paper, enhance privacy and security protection or expose new loopholes?



Integrating HIPAA Privacy and Security, cont'd

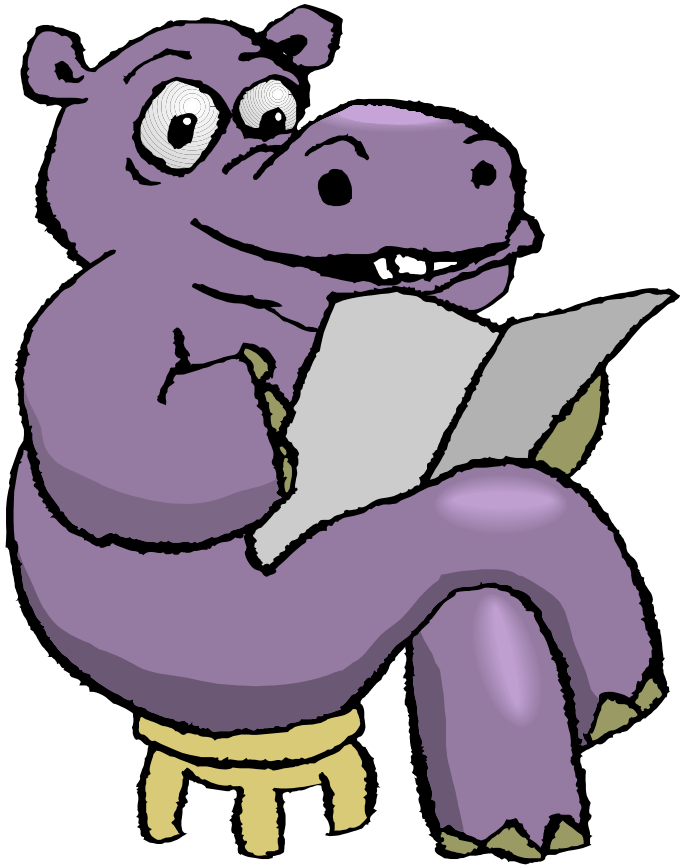
- Are the current HIPAA rules and enforcement mechanisms strong enough to protect privacy and security?
- Is there a need for stronger and more standardized enforcement? (If the rules are scalable, then entities have varying methods of protections.)
- How will issues of preemption affect standardization?

Integrating HIPAA Privacy and Security, cont'd

- Should the National Patient Identifier Rule be finalized?
- How can access and role-based authorizations be standardized across regional or local collaboratives?
- What lessons from educating citizens on the HIPAA Privacy Rule can be learned with the move to Personal Health Records?

Integrating HIPAA Privacy and Security, cont'd

- What about security protections in remote devices such as PDAs and wireless laptops?
- Others????



Questions?

Thank You