

# MMIS 2007 Conference

## San Diego, CA

### *Privacy and Security of Medicaid Data in Health Information Exchanges*

Panel presenter: LaRah Payne, ScD, MPH, CIPP/G  
Senior Policy Analyst/Privacy Officer  
District of Columbia Dept. of Health  
Medical Assistance Administration

# Privacy Warning for the Decade

- *“Privacy and Security are the Chernobyl that is waiting to happen for the health care industry.”*

William Winkenwerder, MD 2001

# The Real Chernobyl



# A Figurative Chernobyl

- **Meltdown: January 22, 2007**
  - External hard drive missing:
    - 48,000 records on drive
    - 20,000 not encrypted
  
- **Hot Update: February 2007**
  - The true numbers:
    - 535,000 records
    - 1.3 million non-VA physicians

***Not a place you would want to be .***

***. .***



# Another Place You Don't Want to Be

2007	NAME (Location)	TYPE OF BREACH	NUMBER OF RECORDS
Feb. 7, 2007	Johns Hopkins University and Johns Hopkins Hospital (Baltimore, MD)	Johns Hopkins reported the disappearance of 9 backup computer tapes containing personal information of employees and patients, Eight of the tapes contained payroll information on 52,000 past and present employees, including SSNs and in some cases bank account numbers. The 9th tape contained "less sensitive" information about 83,000 hospital patients.	52,000 past and present employees plus 83,000 patients
Apr. 10, 2007	Georgia Dept. of Community Health (Atlanta, GA)	A computer disk containing personal information including addresses, birthdates, dates of eligibility, full names, Medicaid or children's health care recipient identification numbers, and Social Security numbers went missing from a private vendor, Affiliated Computer Services (ACS), contracted to handle health care claims for the state.	2,900,000
July 20, 2007	SAIC (San Diego, CA) <a href="http://www.saic.com/response/">www.saic.com/response/</a>	Pentagon contractor may have compromised personal information. Information such as names, addresses, birth dates, Social Security numbers and health information about military personnel and their relatives because it did not encrypt data transmitted online.	580,000

Source: The Privacy Rights Clearinghouse, Chronology of Data Breaches  
<http://www.privacyrights.org/ar/ChronDataBreaches.htm#2007>

# Where We Want to Be

- A full and active participant in developing statewide HIE efforts
- A key facilitator of providers' participation, especially for vulnerable populations, and
- Effectively using Health IT to improve the quality and health outcomes of Medicaid recipients
  - . . . *near the leading edge of technology*

# Questions for the Journey

- Are Medicaid HIE efforts inherently stronger or weaker than other HIE efforts?
- How do we build sufficient privacy and security safeguards into Medicaid HIE efforts?
- How much is “enough” privacy and security to ensure trust in the Medicaid HIE effort?
- What are the specific regional and national issues that affect the development of viable privacy and security solutions?

# Evolving Issues

## □ HIPAA Privacy Principles

- Uses and Disclosures
- Notice (NOPP)
- Access
- Security
- Amendments
- Administrative Requirements
- Authorization

## □ Privacy and Security Domains

- User and entity authentication
- Authorization & access control
- Patient & Provider identification
- Transmission security
- Information protection
- Information audits
- Administrative & physical safeguards
- State law
- Use and disclosure policy

Sources: GAO Analysis of HIPAA Privacy Rule, GAO-07-238, January 2007  
Testimony by Robert Kolodner, MD before House Subcommittee, June 19, 2007

# Health Information Exchange Scenarios (18)

- Treatment (4)
- Payment
- RHIO
- Research
- Law Enforcement
- Prescription Drug Use/Benefit (2)
- Healthcare (2)  
Operations/Marketing
- Bioterrorism
- Employee Health
- Public Health (3)
- State Government Oversight

# Government Efforts on Privacy & Security

Name	Focus Description	Link
American Health Information Community (AHIC). Includes the Confidentiality, Privacy and Security (CPS) Workgroup.	AHIC makes recommendations to HHS on key health IT strategies. The CPS Workgroup makes recommendations to the Community regarding the protection of personal health information in order to secure trust, and support appropriate interoperable electronic health information exchange.	<a href="http://www.hhs.gov/healthit/ahic">www.hhs.gov/healthit/ahic</a> <a href="http://www.hhs.gov/healthit/ahic/confidentiality">www.hhs.gov/healthit/ahic/confidentiality</a>
Best Practices for State HIE Initiatives	Gather information from existing state-level Health Information Exchanges and define, through a consensus-based process, best practices, including privacy and security practices.	<a href="http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_032792.pdf#page%3D5">http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_032792.pdf#page%3D5</a>
Centers for Medicare and Medicaid Services (CMS) Medicaid Information Technology Architecture (MITA) Initiative	CMS/MITA security and privacy activities to: identify the basic MITA security and privacy principles; align security and privacy with the MITA enterprise architecture; define the MITA security and privacy standards; identify security and privacy use case scenarios; outline the relationship between security and privacy goals and policies, and ; create the Subject Area Model	<a href="https://www.cms.hhs.gov/MedicaidInfoTechArch/Downloads/mitasecurity.pdf">https://www.cms.hhs.gov/MedicaidInfoTechArch/Downloads/mitasecurity.pdf</a>
Certification Commission for Healthcare Information Technology (CCHIT)	Develop certification criteria for electronic health records and networks.	<a href="http://www.cchit.org/">http://www.cchit.org/</a>
Health Information Security and Privacy Collaboration (HISPC)	(1) assess variations in organization-level business policies and state laws that affect health information exchange; (2) identify and propose practical solutions, while preserving the privacy and security requirements in applicable Federal and state laws; and (3) develop detailed plans to implement solutions to identified privacy and security challenges.	<a href="http://healthit.ahrq.gov/portal/server.pt?open=512&amp;objID=650&amp;PageID=0&amp;parentname=ObjMgr&amp;parentid=106&amp;mode=2&amp;dummy=">http://healthit.ahrq.gov/portal/server.pt?open=512&amp;objID=650&amp;PageID=0&amp;parentname=ObjMgr&amp;parentid=106&amp;mode=2&amp;dummy=</a>

Source: Internet source documents identified in Link column.

# Government Efforts on Privacy & Security

(continued)

Name	Focus Description	Link
Healthcare Information Technology Standards Panel (HITSP)	Identify standards for use in enhancing the exchange of interoperable health data and harmonize the standards necessary to allow for the protection of the privacy and security of health data.	<a href="http://www.ansi.org/standards_activities/standards_boards_panels/hisp/hitsp.aspx?menuid=3">http://www.ansi.org/standards_activities/standards_boards_panels/hisp/hitsp.aspx?menuid=3</a>
National Committee on Vital and Health Statistics (NCVHS) with its Subcommittee on Privacy and Confidentiality	Developed a report based on a series of five hearings addressing: (A) definitions; (B) the importance of privacy and confidentiality; (C) the role of individuals; (D) controlled disclosure of personal health information; (E) regulatory issues; (F) secondary uses of personal health information; and (G) establishing and maintaining public trust.	<a href="http://www.ncvhs.hhs.gov/060622lt.htm">www.ncvhs.hhs.gov/060622lt.htm</a>
Nationwide Health Information Network (NHIN)	Develop prototypes capable of demonstrating potential solutions for nationwide health information exchange	<a href="http://www.hhs.gov/healthit/healthnetwork/">http://www.hhs.gov/healthit/healthnetwork/</a>
Office for Civil Rights (OCR) HIPAA Oversight and Enforcement	OCR is designated as the agency to monitor compliance with the HIPAA Privacy Rule.	<a href="http://www.hhs.gov/ocr/hipaa/">http://www.hhs.gov/ocr/hipaa/</a>
State Alliance for e-Health (State Alliance) Includes the Health Information Protection taskforce which is responsible for examining privacy and security issues.	(1) identifying, assessing and, through the formation of consensus solutions, mapping ways to resolve state-level health IT policy issues that affect multiple states and pose challenges to interoperable electronic health information exchange; (2) providing a forum in which states may collaborate so as to increase the efficiency and effectiveness of the health IT initiatives that they develop; and (3) focusing on privacy and security policy issues surrounding the use and disclosure of electronic health information.	<a href="http://www.nga.org/portal/site/nga/menuitem.1f41d49be2d3d33eacdcbeeb501010a0/?vgnnextoid=5066b5bd2b991110VgnVCM1000001a01010aRCRD">http://www.nga.org/portal/site/nga/menuitem.1f41d49be2d3d33eacdcbeeb501010a0/?vgnnextoid=5066b5bd2b991110VgnVCM1000001a01010aRCRD</a>

Source: Internet source documents identified in Link column

# Help with Future Challenges

- Standards for interoperability
- Develop privacy and security “use cases” embedding privacy and security into the business processes
- Harmonize differences among interpretations of HIPAA and state privacy laws
- Harmonize rules for information disclosure among categorical gov’t programs
- Medical identify theft safeguards
- Enforcement and sanctions standards

# Guidance for the Next Decade

- *“Privacy is going to be our greatest hurdle, and we must protect it in order to succeed.”*
  - William Winkenwerder, MD
  
- *“Through a series of small steps, the larger goals of health information exchange can be realized.”*
  - Jonah Frohlich, Sam Karp, Mark Smith, MD, Walter Sujansky, MD, PhD

# More Steps on the Journey



- From the American Health Information Community/CPS:  
*All persons and entities, excluding consumers, that participate directly in, or comprise, an electronic health information exchange network, through which individually identifiable health information is stored, compiled, transmitted, modified, or accessed should be required to meet enforceable privacy and security criteria at least equivalent to any relevant HIPAA requirements (45 CFR Parts 160 and 164).*

Source: June 12, 2007 letter from Kirk Nahra Chair, AHIC Confidentiality, Privacy, and Security Workgroup to DHHS Secretary Michael Leavitt.

# *Thanks for Listening*



## □ Contact Information:

- LaRah Payne, ScD, MPH, CIPP/G
- Senior Policy Analyst/MAA Privacy Officer
  
- D.C. Dept. of Health/MAA
- 825 N. Capitol St. NE, Suite 5200
- Washington, DC 20002-4210
- Tel: 202.442.9116
  
- E-mail: [LaRah.Payne@dc.gov](mailto:LaRah.Payne@dc.gov)