

# **NC HIE Council Policy Development Committee**

**NCHICA  
Research Triangle Park, NC  
March 25, 2009**

## AGENDA

<b><u>Start</u></b>	<b><u>Topic</u></b>	<b><u>Discussion Leader</u></b>
11:00	Welcome and Introductions	Dave Dillehunt Kris-Shae McCall
	Policy Landscape	Dave Dillehunt
11:15	American Recovery & Reinvestment Act Policy Issues	Gail Hinte & All
11:45	Working Lunch	All
12:30	Action Plan	All
12:45	CDC – Inter Organizational Agreement project with SC and NC	All
1:00	Adjourn	

# Policy Landscape

- Consumer Centric Policy Considerations
  - Personal Health Records
  - NC Policy Implications
    - Action Plan?

# ARRA HIPAA Privacy & Security

- New definitions:
  - Electronic Health Record
  - Breaches
  - Personal Health Records

# **Title XIII of Division A**

## **Subtitle D**

### ***HIPAA***

# HIPAA Summary

- Federal privacy and security laws (HIPAA) were expanded to protect patient health information, including:
  - Defines which actions constitute a breach (including some inadvertent disclosures)
  - Expands role of protection of PHI to business associates
  - Imposes restrictions on certain disclosures, sales, and marketing of protected health information
  - Requires an accounting of disclosures to a patient upon request
  - Authorizes increased civil monetary penalties for HIPAA violations
  - Grants authority to state attorneys general to enforce HIPAA

*Most HIPAA modifications are effective February 17, 2010*

Analysis by  HIMformatics

# Major Modifications to HIPAA Rules

Area	Major Changes	Effective Date
Business Associates Agreement	<ul style="list-style-type: none"> <li>• Business Associates now regulated (e.g., accountants, attorneys, vendors, consultants)</li> <li>• All BAs must comply with the HIPAA Security rule provisions mandating administrative, physical, and technical safeguards</li> <li>• BAs now subject to the same civil and criminal penalties as covered entities</li> <li>• BAs must have a formal compliance program</li> </ul>	Feb 2010
Security Breach Notification	<ul style="list-style-type: none"> <li>• First national data security breach notification law for both covered entities and BAs to report breaches of “unsecured” PHI*</li> <li>• Notification must be provided to affected individual within 60 days of the discovery of the breach; an annual log must be kept and submitted to HHS</li> <li>• If more than 500 individuals are affected, notice must be provided to “prominent media outlets” and HHS</li> <li>• Same notification requirements for PHR vendors – but will be regulated by the FTC</li> <li>• Interim regulations developed by HHS and FTC by 4/17/09</li> </ul>	9/17/09 (30 days after interim regulations published)

*\*Definition of “unsecured PHI” still to be defined (4/18/09). If deadline passes, definition will be “PHI that is not secured by a properly accredited technology standard. A technology standard I is one that (1) renders PHI unusable and unreadable to unauthorized individuals and (2) is developed and endorsed by standards developing organization accredited by ANSI*

Analysis by



# Major Modifications to HIPAA Rules

Area	Major Changes	Effective Date
Use and Disclosure of PHI	<ul style="list-style-type: none"> <li>• Except for limited purposes (e.g., public health), covered entities may not directly or indirectly receive any remuneration in exchange for an individual's PHI, unless the individual signed an authorization.</li> <li>• Places additional restrictions on a covered entity making certain communications about products or services, where entity receives payment in exchange for communication.</li> <li>• Tightens up definition of "minimum necessary", which in the past had been left to the judgment of the covered entity (Until HHS finalizes definition, the covered entity and BAs will determine the "minimum necessary "disclosure")</li> </ul>	Feb 2010 except for "minimum necessary" which is 8/17/2010
Increased Individual Rights	<ul style="list-style-type: none"> <li>• Covered entity cannot share information with the patient's health plan if provider was paid in full "out-of-pocket"</li> <li>• Covered entity's fundraising communications must provide clear opportunity for individual to opt out of future communications.</li> <li>• Entities maintaining EHRs must provide copies to patients, if requested</li> <li>• Entities maintaining EHRs must provide an accounting of all PHI disclosures for treatment, payment and "healthcare operations" during the prior three years</li> </ul>	Feb 2010 for all but last bullet; see Note for more information

*Note: Timeframes for accounting will vary depending on entities EHR status. If an EHR was acquired before 1/1/09, accounting requirement is effective 1/1/14 to monitor disclosures since 1/1/11. If acquiring an EHR after 1/1/09, requirement is effective on the latter of 1/1/11 or the date of the EHR*

Analysis by



# Major Modifications to HIPAA Rules

Area	Major Changes	Effective Date
Heightened HIPAA Enforcement	<ul style="list-style-type: none"> <li>• Requires periodic audits of covered entities and BAs for HIPAA compliance</li> </ul>	Feb 2010
	<ul style="list-style-type: none"> <li>• Establishes a tiered system of civil penalties based on the nature of improper conduct (unknowing violations, reasonable cause, willful neglect)               <ul style="list-style-type: none"> <li>* Maximum penalty of \$50,000 per violation, up to \$1.5M per year for each violation</li> </ul> </li> </ul>	Immediate
	<ul style="list-style-type: none"> <li>• Civil and criminal liability for HIPAA violations extended to BAs</li> </ul>	Immediate
	<ul style="list-style-type: none"> <li>• Affected individuals may share in penalties collected/ GAO to issue report on the methodology to be utilized for allowing individuals to share in civil monetary penalties imposed by HIPAA</li> </ul>	August 2010
	<ul style="list-style-type: none"> <li>• State Attorney Generals authorized to bring civil actions to enforce HIPAA</li> </ul>	Immediate

# ARRA Timeline: Standards & Regulations

Legend:



**Feb 16, 2009**  
ARRA  
Enacted – HIE funding, R&D grants

**April 18, 2009**  
HHS guidance on methods and technologies that render information unreadable

**By May 18, 2009**

- HIT policy recommendations to ONC re: standards, implementation specifications, and certification criteria
- NIST pilot test of standards and implementation
- Draft description of program to develop regional centers for HIT implementation assistance

**By Aug 16, 2009**  
HHS/FTC final regs on notification of breaches; applies to PHRs breaches not covered by HIPAA or BA agreements

**By Dec 31, 2009**  
HHS adopts initial standards, implementation specifications and certification criteria, including accounting for disclosures

After 1/2010 Grants to states and Indian tribes for EHR loan programs

2/16/09 HIPAA violation penalties (\$50K per up to \$1.5M); enforcement by State Attorneys General for offenses

Medicare (4 yrs) / Medicaid (6 yrs) incentive payments begin

Due by Feb 17, 2010

- Covered entities must enter into BA agreements with PHRs, HIEs, and other services that handle PHI
- Rules to opt out of fundraising solicitations
- Privacy & security requirements for PHR's
- Misc other reports and education initiatives

**Feb 17, 2010**

- Clarification of criminal penalties for non-covered entities
- HHS rules on entities required to be business associates
- Right to restrict disclosures to health plans for out-of-pocket services
- HHS to conduct periodic audits of entities covered by HIPAA
- Right of electronic access of records by patient

**Aug 17, 2010**

HHS guidance on minimum necessary data and regulations regarding sale of data prohibition

Aug 17, 2010 Regulations on sale of data prohibition go in effect

**By Oct 1, 2010**

Report to Congress on available open source HIT systems

**Feb 17, 2011**

Clarification of ability to pursue civil penalties when criminal penalties not pursued

After 10/2010 State grants to promote HIT (implementation grants for HIE), incl req'd matches

By 2014  
GAO to report impact of ARRA

**Jan 2013**  
Accounting and disclosure rules for EHR acquisitions after 1/2009 (extended deadline)

Medicare non-compliance penalties begin

**Jan 2016**  
Accounting and disclosure rules for EHR acquisitions before 1/2009 (extended deadline)

By 2012 Regulations for methodology to distribute penalties or settlement money to harmed individuals

# ARRA Timeline for Privacy Provisions

- Upon enactment (February 16, 2009)
  - Application of new tiered civil penalties based on the nature of HIPAA violations, up to \$50,000 per violation and an annual maximum of \$1.5 million (Section 13410)
  - Enforcement by State Attorney Generals for offenses occurring post enactment (Section 13410e)
- Within 45 days of enactment (April 3, 2009)
  - Appointment of HIT Policy Committee members (Section 3002b)
- Within 60 days of enactment (April 18, 2009)
  - HHS Secretary will issue guidance on methodologies and technologies that render information unreadable (Section 13402)
- Within 180 days of enactment (August 16, 2009)
  - HHS and the Federal Trade Commission will promulgate interim final regulations on notification of breaches. The FTC rules will apply to breach notification by PHRs that are not covered by HIPAA or Business Associate agreements (Section 13402, 13407)
- By December 31, 2009
  - HHS must adopt through rulemaking the initial prioritized set of standards which should include the accounting for disclosures (Section 3002b)
- Due within one year post enactment (February 17, 2010)
  - The Secretary will appoint a Chief Privacy Officer (Section 3001)
  - The Office of Civil Rights and HHS will launch an education initiative to improve public transparency on the use of health information (Section 13403)
  - The Government Accountability Office will report on best practices for disclosures for treatment and use of electronic informed consent (Section 13424)
  - HHS will report on and provide guidance on de-identification (section 13424c)
  - Covered entities must enter into Business Associate Agreements with PHRs, HIEs, and other services that handle projected health information (Section 13405e)
  - HHS will issue rules on opting out of fundraising solicitations (Section 13406)
  - HHS will report on guidance on the effective technical safeguards for carrying out the HIPAA security rule (Section 13401c)
  - HHS and the Federal Trade Commission will report on privacy and security requirements for PHR vendors and applications

Analysis by



# ARRA Timeline for Privacy Provisions

- One year post enactment (February 17, 2010)
  - HHS and the Office of Civil Rights clarify application of criminal penalties for non-covered entities (Section 13409)
  - HHS to issue rules on which entities are required to be business associates (Section 13401)
  - Right to restrict disclosures to health plans for services paid for out of pocket (Section 13405a)
  - HHS Secretary required to conduct periodic audits of entities covered by HIPAA (Section 13411)
  - Right of electronic access of records by patients takes effect (Section 13405e)
- Within 18 months of enactment (August 17, 2010)
  - HHS guidance on minimum necessary data (Section 13405c)
  - Regulations regarding sale of data prohibition which take effect 6 months post promulgation (Section 13405a)
- By 2011
  - Initial deadline for complying with new accounting and disclosure rules for information kept in EHRs acquired after January 1, 2009 (Section 13405c)
- 24 months post enactment (February 17, 2011)
  - Clarification of ability to pursue civil penalties when criminal penalties are not pursued (Section 13405)
- By 2012
  - Regulations for methodology for distributing penalties or settlement money to harmed individuals (Section 13410)
- By 2013
  - Extended deadline for complying with new accounting and disclosure rules for information kept in EHRs acquired after January 1, 2009 (Section 13405c)
- By 2014
  - GAO will report on the impact of ARRA (Section 13424)
  - Initial deadline for complying with new accounting and disclosure rules for information kept in EHRs acquired before January 1, 2009 (Section 13405c)
- By 2016
  - Extended deadline for complying with new accounting and disclosure rules for information kept in EHRs acquired before January 1, 2009 (Section 13405c)

# Recommended Next Steps

Area	Next Steps
Business Associates Agreement	<ul style="list-style-type: none"> <li>• Expand BA lists to include vendors and others involved in handling PHI</li> <li>• Re-evaluate relationships which require BA agreements</li> <li>• Revise current BA Agreement to require BAs to develop and maintain Compliance Plan</li> <li>• Develop process to annually obtain information from BAs to confirm HIPAA compliance</li> </ul>
Security Breach Notification	<ul style="list-style-type: none"> <li>• Develop breach notification process</li> <li>• Evaluate if current “technology standard” avoids notice requirements</li> <li>• Be informed of technology standards will be defined if HHS does not meet 4/18/09 deadline</li> </ul>
Use and Disclosure of PHI	<ul style="list-style-type: none"> <li>• Define current “minimum necessary” definition until final definition issued</li> <li>• Re-evaluate marketing policy using PHI</li> </ul>
Increased Individual Rights	<ul style="list-style-type: none"> <li>• Re-evaluate policies on accounting for PHI disclosures;</li> <li>• Determine how to provide electronic records to requesting individuals</li> <li>• Begin accounting for disclosures as early as 1/1/11</li> <li>• Modify fundraising letter</li> </ul>
Heightened HIPAA Enforcement	<ul style="list-style-type: none"> <li>• Conduct security “check-up” to ensure appropriate processes are in place prior to an HHS HIPAA audit (including workforce training and BA’s compliance)</li> <li>• Ensure that all policies, procedures and related forms reflect the new requirements</li> </ul>

# Next Steps

- Action Plan
  - Policies to Enable HIE Across NC
  - Readiness for Stimulus Bill Requirements
    - Assessment
      - Physicians
      - Hospitals
      - Other Providers / Covered Entities
  - Business Associates vs Covered Entities
    - Form Adjustments?
  - Cash Transactions – Procedures to Manage
  - TPO Audit Trail
  - Minimum Data Set – Definition and Actions

# CDC IOA Report

- Purpose
  - Sharing Bio Surveillance Data Across North Carolina and South Carolina Border - Charlotte
- Progress
  - First Phase of Regional CDC Region IV
  - Data Sharing Agreement Negotiated Between North Carolina and South Carolina Public Health
- Assistance Desired from this Committee
- Next Steps

## Upcoming Meetings

- **April 22**                      **11:00 a.m.**    **NCHICA Offices**
- **May 27**                        **11:00 a.m.**    **NCHICA Offices**