



Will Privacy & Security Concerns Impede HIT Initiatives?

HIPAA and HIT Summit

March 28, 2007

Bill Braithwaite, MD, PhD
Health Information Policy Consulting
Washington, DC

Value of Interoperable HIE

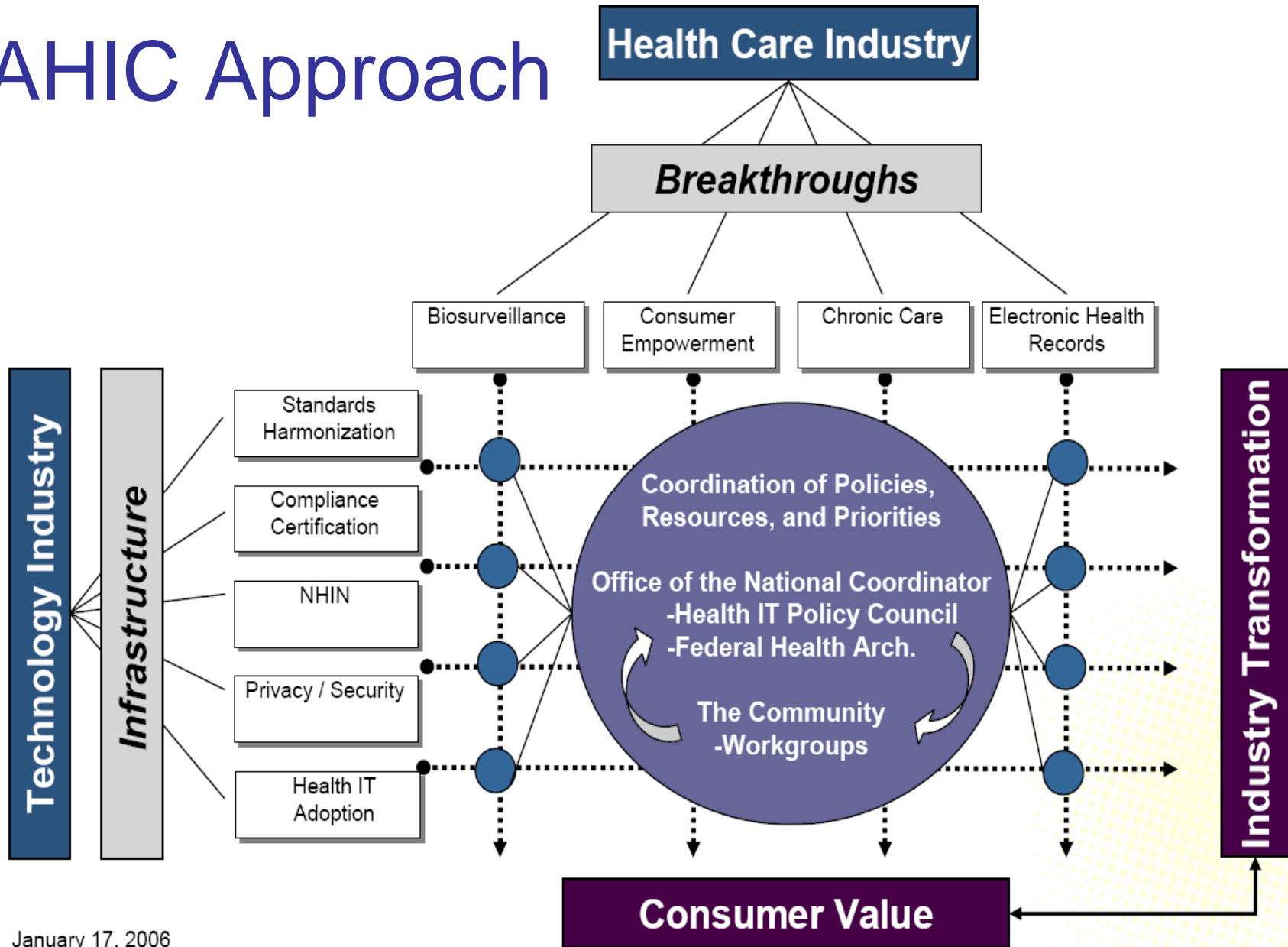
- Standardized, encoded, interoperable, electronic, clinical HIE saves money*:
 - Net Benefits to Stakeholders of \$78B/yr.
 - Providers - \$34B
 - Payers - \$22B
 - Labs - \$13B
 - Radiology Centers - \$8B
 - Pharmacies = \$1B
 - Reduces administrative burden of manual exchange.
 - Decreases unnecessary duplicative tests.
- HIE + EHR + CDSS => SAVES LIVES!

*From Center for Information Technology Leadership, 2004

American Health Information Community (AHIC)

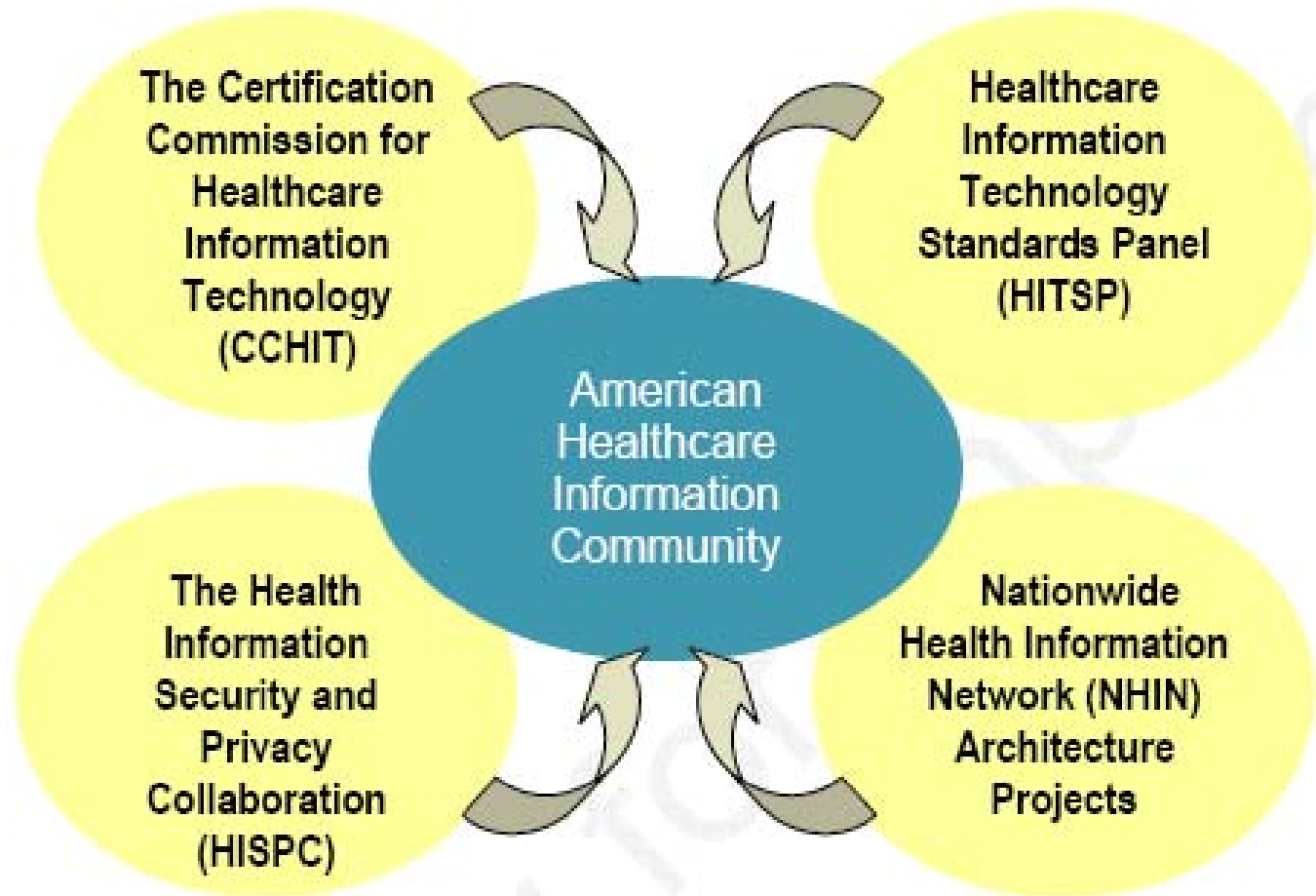
- Formed in September 2005 under the auspices of FACA.
- Provides recommendations to HHS on how to make health records digital and interoperable, and assure that the privacy and security of those records are protected, in a smooth, market-led way.
 - www.hhs.gov/healthit/ahic.html
- 18 Commissioners – consumer groups, providers, payers, hospitals, vendors, government (50-50 split) – Chaired by Secretary Leavitt and now with David Brailer as Vice-Chair.
- Dissolution within two to five years with goal of creating self-sustaining, private sector replacement
- First meeting October 7, 2005.
- Recent meeting March 13, 2007.
- Next meeting April 24, 2007.

AHIC Approach



January 17, 2006

ONC Contracts to Support AHIC



Privacy & Security Contract

aka Health Information Security and Privacy Collaboration (HISPC)

- Assess variations in organization-level business policies and state laws that affect health information exchange.
- Identify and propose practical solutions, while preserving the privacy and security legal requirements.
- Develop detailed plans to implement solutions.
- Coordinate through NGA and subcontracts with 34 states or territorial governments.
 - Directly teaming in this manner is a critical element to the successful completion of this contract within the prescribed timeframe.
- Contract to RTI International for 18 months, \$11.5M.
 - Subcontracts for < \$350K.

Health Information Security and Privacy Collaboration (HISPC)

- 33 State and 1 Territory contracted (June-July)
- 10 Regional Meetings (43 states participated)
- Interim Reports
 - Assessment of Variation (November 2006)
 - Analysis of Solutions (January 2007)
 - Implementation Plans (February 2007)
- National Meeting (March 2007)

National Meeting (March 2007)

- Day 1: 4 Tracks
 - Consent
 - Data Security and Quality
 - Legal and Regulatory Issues
 - Interpreting and Applying HIPAA
- Day 2: 4 Tracks
 - Reducing Mistrust through Education and Outreach
 - Moving Forward in States at Different Points in the Process
 - Governance and Implementation
 - State Legislation and Business Policies

Participants Vary on Key Dimensions

- Degree of adoption of electronic HIE.
 - Several states have sophisticated and functional systems of eHIE.
 - coverage is far from universal.
 - Many states lack working eHIE models.
 - must imagine issues and consequences from paper-based experiences.
- Legal and regulatory conditions.
 - Laws and regulations evolved in response to paper exchanges.
 - Legal strictures dispersed across many different laws.
 - sometimes inconsistent with one another.
 - Many laws silent with respect to eHIE.
 - leads to varied business practices and customs.
- Demographic composition of the state.
 - population size,
 - cultural and ethnic diversity,
 - geographic dispersion.
- Health care market forces in the state.
 - Business and organizational dynamics and relationships between health care entities affect the ways in which HIEs are adopted and implemented.
- This diversity challenges summary!

WY Variations

- Inconsistent and incorrect interpretation of HIPAA
 - No authoritative interpreting body exists
 - Smaller facilities lack resources to interpret law
 - Fear of legal reprisal for wrongful disclosure engenders conservative practices
- Lack of existing electronic health information infrastructure
 - EHRs exist but are not interoperable
 - Concerns over security, privacy, cost, and complexity deter many providers and consumers from HIT adoption
 - Most providers resist centralized or mandated systems
- Outdated state statutes inhibit exchange of health information
 - Recently passed “credit freeze” laws protect financial information, but do not specifically address health information
 - Existing health privacy laws only apply to in-patient facilities

WY Proposed solutions

- HIPAA interpretation => establish an HIE research and policy coordinating center for Wyoming
 - Analyze, clarify, and communicate legal and technical issues
 - Provide education and training
- Lack of infrastructure => create an HIE pilot project
 - Develop an interface mechanism for information exchange among disparate systems
 - Demonstrate benefits and trustworthiness of HIE to providers and consumers
- State statutes => generate changes in state law
 - Extend protection and notification laws to health records
 - Review and update several statutes to assure consistency
 - Address other specific needs such as high-risk juveniles

WY Implementation plans

- HIE research and policy coordinating center
 - Wyoming Health Information Organization (WyHIO) will house the center
 - Initial tasks
 - Appoint an advisory board to determine mission
 - Develop a business plan and seek funding
 - State support
 - Membership model (Utah Health Information Network)
 - Goals
 - Provide consistent and clear interpretations of HIPAA, particularly for small rural facilities without legal advisors
 - Act as a non-vendor advocate for HIT
 - Support multidisciplinary research and education

WY Implementation plans

- HIE pilot project
 - WyHIO will also be responsible for this project
 - Initial tasks
 - Complete a preliminary network design and a basic application area (medications, trauma or secondary/specialty care)
 - Identify funding sources (a bill in 2007 Wyoming Legislature that proposed \$4,000,000 for a project died in committee)
 - Contract with a developer to create a prototype
 - Work with existing or developing EHR systems
 - Goal: demonstrate feasibility of non-centralized HIE and build trust among providers and consumers

WY Implementation plans

- State statutes
 - Work with legislator and attorney stakeholders to draft changes and/or enact new bills for 2008 Wyoming Legislature
 - Create a health information privacy law requiring notification of all consumers affected by a compromise of health records
 - Update Wyoming Hospital Records and Information Act and Wyoming Public Records Act to address inconsistencies with HIPAA and each other
 - Will require a study to evaluate laws and effects of change
 - Create a health information exchange act to define who is allowed to share information about juveniles, particularly in high-risk situations or matters of public health/safety

NJ Barriers

- Identification of the Patient
 - Master-Patient Index is one of 14 necessary foundation blocks for RHIO to interoperate
 - Solution in Health ID Cards with Bar Coding or Electronic Strip
- Understanding and Resolving Legal and Policy Issues
 - Especially Consent Management and Sensitive Data Controls

NJ Identification of the Patient

- NJ State and Regional Master Patient Index [MPI]
 - Unique ID
 - Cross walked to legacy numbers
 - Assigned:
 - At birth
 - At hospital / ED admission
 - Upon patient request
 - Goal: reliably link each NJ patient with their health care record
 - Opt-out permitted
 - No longer part of EHR /RHIO
 - Payment may be delayed

MN Privacy Barriers to HIE

- Patient consent required for nearly all disclosures of health records – **including treatment**
 - Patients need to give written consent
 - Consent generally expires within one year
 - Limited exceptions to consent
 - Medical emergency
 - Within “related” health care entities
 - Consents that do not expire
 - Disclosures to providers being consulted
 - Disclosures to payers for payment

MN Privacy Barriers to HIE

- Minnesota law places all liability for inappropriate disclosures on the disclosing provider:
 - A violation of patient consent requirements may be grounds for disciplinary action
 - A person who negligently or intentionally releases a health record is liable to the patient for compensatory damages, plus costs and fees
- Providers are very cautious in disclosing data and respond to privacy/security concerns by not disclosing patient data

MN Causes of Patient Consent Barriers

- **Undefined terms and ambiguous concepts** that are used in Minnesota Statutes § 144.335 - patient consent requirements
- Difficulties in determining the **appropriate application of consent requirements to new concepts** in the electronic exchange of health information that do not have an analogous concept in a paper-based exchange
- The **need to update consent requirements to allow mechanisms that facilitate the electronic exchange** of patients' information while respecting the patients' ability and wishes for controlling their information

MN Generating Solutions

- A workgroup of industry representatives and privacy advocates did not reach consensus on solutions:
 - Identified options
 - Documented advantages and disadvantages for each option
 - Connected related options
- MDH developed criteria for evaluating options:
 - maintain or strengthen patients' privacy or control over their health records
 - improve patient care
 - facilitate electronic, real time, automated exchange
 - not place an undue administrative burden on the health care industry
 - increase the clarity and uniform understanding of the statutory language and consent requirements

MN Legislative Solutions

- **Statutory Modifications for Legislative Consideration**
 - Clarify undefined terms and ambiguous concepts:
 - “Health Record”
 - “Medical Emergency”
 - “Related Health Care Entity”
 - “Current Treatment”
 - Apply consent requirements to new concepts:
 - “Record Locator Service”
 - “Identifying Information”

MN Legislative Solutions (cont)

- **Statutory Modifications for Legislative Consideration**
 - Update mechanisms that facilitate electronic exchange:
 - Create ability of a provider to rely on another provider's representation of having obtained consent
 - Develop a legal framework for allocating liability between disclosing and requesting providers
 - Permit representation of consent to be transmitted electronically when requesting patient information
 - Recodify Minnesota's patient consent statutes to make the requirements easier to understand for patients and health care providers

HISPC Sources of Variation

- Variation related to misunderstandings and differing applications of federal laws and regulations
 - HIPAA Privacy Rule
 - Patient Authorization/Consent
 - Variation in Determining “Minimum Necessary”
 - HIPAA Security Rule
 - Confusion regarding the different types of security required
 - Misunderstandings regarding what was currently technically available and scalable
 - CFR 42 part 2
 - Variation in the treatment facilities’, physicians’, and integrated delivery systems’ understanding of 42 C.F.R. pt. 2, its relation to HIPAA, and the application of each regulation

HISPC Sources of Variation (continued)

- Variation related to state privacy laws
 - Scattered throughout many chapters of law
 - When found, they are often conflicting
 - Antiquated--written for a paper-based system
- Trust in applied information security
 - Organizations of each other
 - Consumers/Patients trust of others
- Cultural and business issues
 - Concern about liability for incidental or inappropriate disclosures
 - General resistance to change

Major Categories of State Solutions

- Governance — Most call for a permanent body to oversee and guide implementation of privacy and security solutions.
- Business practices and policies solutions — Most call for standardization (using model forms, contracts, policies, and processes) of business practices for:
 - consent and authorization,
 - application of federal law,
 - exchange of sensitive information, and
 - exchange of data related to Medicaid, public health, and law enforcement agencies.

Major Categories of State Solutions

- Legal and regulatory solutions — Most call for amending state law and introducing new legislation where required.
- Technological solutions — Most call for standardized approaches to:
 - patient identification systems;
 - authorization, authentication, access, and audit;
 - segmenting data within electronic medical records;
 - terminology standards; and
 - transmission security standards.
- Education and outreach — All call for both consumer and provider education and outreach.

HISPC Implementation Plans

- Practical approaches and actionable steps for implementing solutions (due April 2007)
 - Actions
 - Governance and Leadership
 - Realignment of teams
 - Resources required
 - Funding
 - Staffing
 - Timelines
- Nationwide Summary (due June 30, 2007)

Summary of Results

- **Fear** –
 - Violation of state or federal laws that are not understood.
 - Individuals are fearful of making ‘reasonable’ decisions.
 - Liability (personal and financial).
 - Leads to conservative approach to legal advice.

Summary of Results (cont'd)

- **Uncertainty** –

- Low level of understanding across the range of patients and healthcare employees (including some lawyers).
 - Rights and responsibilities under complex set of laws and regulations.
- Organizations interpret HIPAA “reasonable safeguards” guidelines inconsistently.
 - Enforcement actions are ‘reasonable’ but ‘unknown’.
- Lack of standard set of technology to implement.
 - Variations in communications media create difficulties in information exchange.
 - Non-uniform implementation of encryption and other security technology in electronic methods of information exchange.

Summary of Results (cont'd)

- **Doubt** –
 - Trust – how do I know I can trust my data exchange partners?
 - Issues may be disappearing over time with community discussions.
 - Organization size and associated fiscal constraints.
 - Lack of investments in implementing technologies for information safeguards.
 - Doubt about ROI and/or its timing.

Summary

- Fear, Uncertainty, and Doubt will impede HIE and HIT Initiatives unless resolved.
- States are starting to understand the issues.
- States are formulating solutions:
 - Practice and Policy Solutions.
 - Legal and Regulatory Solutions.
 - Technology and Data Standards.
 - Education and Outreach.
- Multi-state and National Level Recommendations are forthcoming.

Thank you!

William R. “Bill” Braithwaite, MD, PhD
Washington, DC
bill@braithwaites.com