



HEAL 5 Kickoff Meeting

Privacy and Security Workgroup

Co-chairs: Tom Check – VNS of NY
Lisa Santelli – Excellus
Ellen Flink – DOH

Staff: Bill Bernstein – Manatt, Phelps
& Phillips
Katie O’Neill – Legal Action
Center



Privacy and Security Workgroup

Agenda for Today's Breakout Session

- Introductions
- Objectives and process for this session
- Q & A from morning session
- Overview of Privacy and Security Workgroup and Subgroups
- Discuss scope of work, consensus on priorities, charter, timelines, and organization and decision process



Privacy and Security Workgroup Overview



Workgroup Overview

- This workgroup will be initially comprised of 3 subgroups to develop the suite of privacy and security policies, including:
 - Consumer consent and operational and environmental processes to support these policies
 - Authorization, Authentication, Access controls, and Audits (the 4As)
 - Contractual and regulatory framework to enforce these policies



Workgroup Overview (cont.)

- RHIOs have responsibility for ensuring privacy and security of information collected and exchanged via the Statewide Health Information Network for New York (SHIN-NY)
 - Authorization for access
 - Authentication of identity
 - Access controls
 - Audit trails for clinicians and consumers
 - Consumer and provider identification
 - Transmission security
 - Data integrity
 - Administrative and physical security
 - Enforcement and protections



Workgroup Purpose and Scope

- Overview
- Purpose and Scope
 - Protecting privacy, strengthening security, ensuring affirmative and informed consent and supporting the right of New Yorkers to have greater control over and access to their personal health information are foundational requirements for interoperable HIE
 - Statewide collaboration process requires:
 - Develop -- develop policies to enable HIE
 - Operate -- determine operational and environmental processes to support the policies efficiently and accurately
 - Specify -- specify business requirements and solutions to support policies
 - Enforce -- develop contractual and regulatory framework to enforce policies
 - Contractual framework to enforce policies, including: state-level participation agreements and vendor subcontractor requirements
 - Regulatory framework to enforce policies while allowing market innovation, e.g, RHIO accreditation as governance entities



Key Principles of Consent Policies and Procedures

Policies and procedures for consent will:

- Promote patient-centered care by facilitating consumer choice and addressing consumer concerns about privacy
- Promote exchange of comprehensive information ensuring clinical effectiveness to improve the quality and efficiency of care
- Minimize burdens on healthcare providers
- Be practical and “implementable” for RHIO participants providing operational flexibility
- Be simple and clear with a concrete rationale
- Foster innovation while ensuring public trust
- Be neutral on technology model



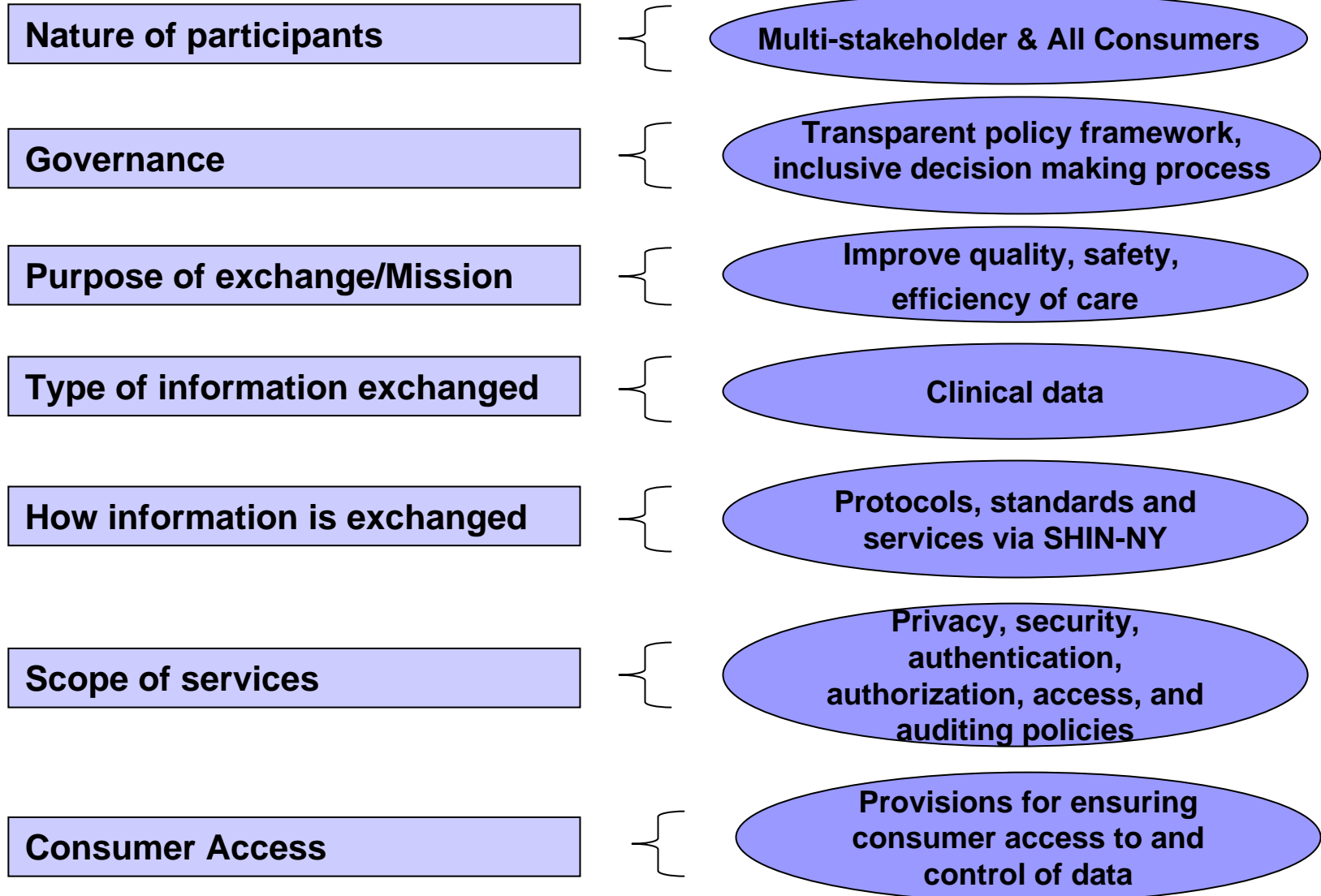
Principles for Affirmative and Informed Consent

- Any New Yorker has the right not to participate in interoperable HIE enabled by the RHIO
- If a patient grants consent to participate, they have a right to allow or prohibit access to their PHI by provider organizations of their choice
- The patient consent allows provider organization to access PHI for permitted uses: treatment, quality improvement and disease management
- The patient consent allows health plans, employers and other third parties to access PHI for permitted uses: quality improvement and disease management
- Provider organization can then access all PHI, including sensitive information from all providers participating in interoperable HIE
- Patient is informed about all participating providers in the RHIO and how updates to the participant list can be obtained
- Patient gives consent at the provider organization level and allows access to patient's PHI by all authorized individuals in the organization to the extent needed
- Permitted uses are limited to treatment, quality improvement and disease management



Analytic Framework

RHIO – Core Components





Consumer Consent Implementation and Harmonization Subgroup



Consumer Consent Implementation and Harmonization Subgroup

- Advance health information exchange via the SHIN-NY through the development and implementation of a standardized, clear and consistent consent process for RHIOs in NYS
- Address outstanding issues including previous recommendations
 - One to one exchange
 - Break the glass
 - Provider Organizations
 - Minors
 - Workflow issues
 - Independent physician practices
 - Care management
 - Federally qualified alcohol and substance abuse facilities
 - Use of de-identified data exchanged through RHIOs



Consumer Consent Implementation and Harmonization Subgroup (cont.)

- Standardized consent form and educational materials
 - Ensure that consumer consent is informed and knowing
- Operations Guidance to RHIOs Implementing White Paper Provisions
- Give RHIOs standing to address patient consent on behalf of physicians, providers and New Yorkers




Deliverables and Timeline

- Updated White Paper
- Recommendations on outstanding issues
- Recommendations on a standardized consent form
- Finalize as part of full suite of privacy and security policies
- Timetable – Oct. 2008



Authorization, Authentication, Access Controls and Auditing (4As) Subgroup



Authentication, Authorization, Access Controls and Auditing (4As) Subgroup

- Determine statewide 4As policy with which all RHIOs need to comply from a policy perspective and require HSPs from a technical perspective via CHxP protocol
 - Catalogue and assess existing practices
 - Establish statewide 4A policies
 - Determine operational and environmental processes to support 4A policies
 - Specify business and work with Protocol and Services work group on technical requirements and solutions to support 4A policies
 - Enforce 4A policies through contractual and regulatory framework
 - Common language for participation agreements and vendor subcontracts



Deliverable and Timeline

- Develop common statewide policy and procedure guidelines for 4As in conjunction with consent recommendations
- Support Protocols and Services work group on technical requirements
- Timetable - Oct. 2008



Contractual and Regulatory Solutions Subgroup



Contractual and Regulatory Solutions Subgroup

- Proposed policies enforced through HEAL 5 contracts
- Development of regulatory framework as long term solutions
- Consider mechanisms for accountability and enforcement:
 - Promoting compliance
 - Penalizing breaches



Enforcement and Consumer Protections

- RHIOs need to have internal capabilities to audit disclosures and regularly monitor to protect against unauthorized access and use. These capabilities should be common statewide and finalized through the statewide collaboration process.
- RHIOs should designate staff who will oversee privacy and consent management functions.
- RHIOs should also provide ombudsman services to consumers to handle questions and facilitate referral for complaints.
- DOH needs to develop policies regarding RHIO and providers' roles and responsibilities in the event of an unauthorized disclosure, disposition of complaints, consumer notification and access to information about disclosures.
- The consent form and education process should include information about consumer rights with regard to unauthorized disclosure or use, including how to file complaints and what remedies are available.



Enforcement and Consumer Protections (cont.)

- Who assumes responsibility for unauthorized disclosure of data?
- Current responsibilities apply:
 - Provider currently assumes responsibility for breaches of privacy occurring on its connection to the system; RHIO assumes responsibility for breaches committed in region via SHIN-NY node.
- Current notification policies apply:
 - RHIO-level breach: RHIO commits that it will notify providers (and patients) when they discover breaches committed directly in region via SHIN-NY node rather than through a provider.
 - Provider-level breach: Provider required to mitigate the effects of such breach and notify patient as per NYS and Federal law. Provider also commits to notify RHIO of breaches.
- Notification for breaches of data occurring through another RHIO:
 - Breaches involving data from an outside RHIO are required to be reported immediately to the other RHIO.
 - Suspicious activity involving data from an outside RHIO are also required to be reported to the outside RHIO.



Enforcement and Consumer Protections (cont.)

Corrective action and sanctions:

- In the event of a breach involving data from an outside RHIO each RHIO commits it will follow existing intra-RHIO policies for corrective action and sanctioning of users and participants.
- A RHIO whose data is breached through use of another RHIO's tools is permitted access in a timely manner to the results of any investigation around that breach and the plans for corrective action.
- If these terms are not met, a RHIO reserves right to withdraw from data use agreement.



Why a Broad Regulatory Framework is Necessary

- NYSDOH is committing hundreds of millions to develop a health information infrastructure, including the statewide health information network of New York (SHIN-NY).
- Success of SHIN-NY depends upon RHIOs' ability to:
 - Govern statewide HIE policies ensuring consistency and compliance, including privacy & security policies and other health information policies
 - Requiring HSP partners to comply with CHIxP protocols and other standards
- For RHIOs to become trusted stewards, stakeholders need assurance that RHIOs have the necessary characteristics and capabilities to perform required services.



Deliverables and Timeline

- Recommendations on regulatory and statutory framework and mechanism for accountability with statewide policies, including privacy and security policies
 - What can be enforced through accreditation
 - What can be enforced through regulation or legislation
- Timetable – Oct. 2008



Workgroup Charter



Mission

- Mission:
 - Protect privacy, strengthen security, ensure affirmative and informed consent, and support the right of New Yorkers to have greater control over and access to their personal health information as foundational requirements for interoperable HIE
 - Support CHITAs as necessary



Functions, Responsibilities, Deliverables:

- Complete Assessment Of Implementation Issues Associated With Final Consent Policy Paper -> Deliverable = Implementation Assessment Framework
- Review And Provide Feedback On Proposed Consent Form And Any Other Materials Developed To Support Consent Process Implementation -> Deliverable = Policy Input
- Develop Detailed Implementation Guides For RHIOs To Comply With NYS Consent Policies -> Deliverable = Implementation Guides
- Develop Technical Assistance Resources Including Dissemination Of Best Practices -> Deliverables Include A Strategy Based On Priorities Set By Group And Vetted Through POC; Identification And Collection Of Best Practices (Documents, Tools) To Be Made Available Through Collaborative Repository
- Coordinate With Other Workgroups Involved In Development Of Standards And Materials To Ensure Consistency And Alignment Across Implementation Spectrum (Consumer Advocacy Coalition, Education And Communications Committee, Core Services And Protocols Workgroup, Possibly Ehr Collaborative) -> Deliverable = Reflect Comments From Other Groups In All Workgroup Products



Membership Criteria and Interest

- Leaders or staff from RHIO/CHITA projects who can commit their organizations to workgroup decisions
- People with legal, policy or regulatory experience and expertise on privacy and security issues, including those who have been part of the NY HISPC project phases 1 and 2
- Representatives of groups who represent consumer or public interests
- Directors or staff of RHIO/CHITA projects involved with the implementation of these policies
- Clinicians and professionals experienced in workflow/practice design who can advise the workgroup on front-line experience with privacy and security policy decisions
- Diversity of sectors is encouraged and recommended



Consensus on Priorities and Timelines

- Subgroup Chairs
- Frequency of meetings/conference calls
- Deliverables
- Next steps