Minutes

Massachusetts Health Information Technology Council
And Advisory Committee Meeting

June 18, 2012
3:30 – 5:00 p.m.

One Ashburton Place, 21st Floor Conference Room 2
Boston

Minutes
Massachusetts Health Information Technology Council
And Advisory Committee Meeting

June 18, 2012

Attendees:

Council Members:
JudyAnn Bigby, MD – (*Chair) Secretary of Health and Human Services*
Deborah Adair – *Director of Health Information Services/Privacy Officer, Massachusetts General Hospital*
Karen Bell, MD – *Chair of the Certification Commission for Health Information Technology (CCHIT)*
James Ermilio – *Special Council to Secretary Gregory Bialecki, representing EOHED*
Lisa Fenichel, MPH – *E-Health Consumer Advocate*
Julian Harris, MD – *Director of Medicaid, Commonwealth of Massachusetts*
John Letchford – *Chief Information Officer, Commonwealth of Massachusetts*
Abigail Moncrieff, JD – *Peter Paul Career Development Professor and Associate Professor of Law, Boston University School of Law*

HIE-HIT Advisory Committee:
John Halamka, Co-Chair – *Chief Information Officer, Beth Israel Deaconess Medical Center*
Nicolaos Athienites, MD – *Renal Medical Care*
Rita Battles – *Director, Inpatient Services, Department of Mental Health*
Peter Bristol – *Vice President and Chief Technology Officer, Network Health*
Kathleen Donaher (TP) – *Associate Professor, Regis College*
Gillian Haney, MPH – *Department of Public Health*
Deborah Stevens (TP) – *Information Security Officer, Tufts Health Plan*
Barbara Popper (TP) – *Project Director, Federation for Children with Special Needs*
Wendy Mariner – *Edward R. Utley Professor of Health Law, Boston University*
Keith Maxwell – *Technical Services Director, Mass League of Community Health Centers*
John Poikonen – *Pharmacy, UMass Medical School*

(TP) participated by telephone

MTC/MeHI:
Laurance Stuntz – *Director, Mass eHealth Institute*
Pamela Goldberg – *Chief Executive Officer, Mass Technology Collaborative*
Judy Silvia – *Director, Government Affairs/MeHI Chief of Staff*

Rick Shoup – *Chief Technology Officer*
Christopher Andrews – *Chief Financial Officer/Administrative Officer*
Donna Nehme – *Executive Assistant*
Mike Noonan – *Managing Principal, Strategic Health Consulting (MeHI Consultant)*

Other:

David Smith – *Massachusetts Hospital Association*
Claudia Boldman – *Administration and Finance*
Deb Schiel – *EOHHS/MassHealth*
Foster Kerrison – *Royal College of Surgeons of Edinburgh*
Christine West – *Massachusetts eHealth Collaborative*
Micky Tripathi – *Massachusetts eHealth Collaborative*
Helene Solomon – *Solomon McCown & Company*
Mark Belanger – *Massachusetts eHealth Collaborative (MAeHC)*
Piali De – *Senscio Systems*
Kathleen Jones – *TTT Mentor Program*
Venkat Jegadeesan – *Executive Office, Health & Human Services (EOHHS)*

The forty third meeting of the Massachusetts Health Information Technology Council was held on June 18, 2012, at One Ashburton Place, 21st Floor, Conference Room 2, Boston, Massachusetts.

Secretary Bigby called the meeting to order at 3:35 p.m.

I. Approval of the April 30, 2012 Meeting Minutes:

After motions were made, seconded, and approved with no abstentions, it was agreed to accept the draft minutes as the official minutes of the April 30, 2012 meeting.

HIE-HIT Advisory Committee Meeting notes:
*Please refer to Slide Presentation "Health IT Council and Advisory Committee Meeting" June 18, 2012.

II. Introduction of Laurance Stuntz, the new MeHI Director

- Laurance discussed the current state of Health IT in Massachusetts as compared to Strategic Health IT Goals (see slides 3-6)

III. Preliminary MeHI Fiscal Year 2013 Budget Review (see slides 7-18)

- Laurance reviewed the FY12 budget

IV. MeHI Programmatic Review (see slides 27)

V. HIE Advisory Workgroup Report

- The Technology and Implementation WG presented the following recommendations across seven topic areas/categories:

Topic Area	Recommendations
Transport	a) The HIE services will follow/support the following transport standards: SOAP/XDR, S/MIME – SMTP in alignment with national standardization efforts. b) The transport standard should support end-to-end security for messages in line with Encryption recommendations
Encryption/Decryption	a) All data transport is to be secured from sender to receiver. b) Message exchange pattern (e.g., EHR to EHR, EHR to Web Portal, etc…) should determine encryption design
Identity Validation	a) EOHHS should be responsible for performing organization level identity validation for those accessing HIE services. Each organization is responsible for performing individual level identity validation. b) For individuals accessing HIE services, EOHHS should be responsible for performing individual level identity validation. c) Standard operating procedures for identity validation should be developed by EOHHS in conformance with Access, Authorization, and Authentication policies and procedures. Identity validation processes should include identity proofing, authorization validation (for primary access and delegates), and permission verification.
Certificate Assignment	a) In alignment with Data Encryption recommendations, private keys should be assigned at the organization level for individuals accessing HIE services through an organization. b) In alignment with Data Encryption recommendations, private keys should be assigned at the individual level, and managed by EOHHS on behalf of individuals, for individuals accessing HIE services via Web Portal. c) EOHHS should outsource the private key assignment and management to a qualified third party vendor.

Topic Area	Recommendations
Metadata	a) Message metadata should adhere to the Minimal Metadata Definition.* The "required if available" fields (patientID; sourcepatientID; sourcePatientInfo) will not contain unencrypted patient health information (PHI) and organizations will be given the option either to leave these fields unpopulated or to populate these fields with hash values for purposes of patient record matching. b) Origination and destination addresses should be separate from message content to support minimization of PHI access. c) EOHHS and its Technical Services vendor should have access to metadata for messages sent via the Direct gateway. d) Metadata may be unencrypted for the duration required for an address query. * Minimal metadata definition from the Direct Project, XDR and XDM for Direct Messaging Specification
Data Retention for DIRECT enabled EHR	a) Copies of messages sent via the Direct Gateway from one Direct enabled EHR to another Direct enabled EHR should not be retained beyond the time required to confirm that message transaction was completed without error b) A transaction log should be maintained with the following information to support audit policies and procedures: Message ID; Addressing information (in line with metadata recommendation); Date and Time; Confirmation receipt
Data Retention for Webmail	a) The HIE should not perform automatic deletion of messages. b) The HIE should set and communicate limits for webmail storage capacity and message retention times. This is needed to plan for and manage storage capacity and to control associated costs. c) Subject to webmail vendor capabilities, the HIE should offer a tiered service level approach to message retention times and message storage capacity to accommodate different user types and user technical capabilities/maturity. The HIE should offer a base level and tiers above and beyond the base level should be priced to cover the incremental costs of storage. d) Invalid address notifications should be provided to senders that initiate to an invalid address immediately upon attempting to send. e) Subject to webmail vendor capabilities, reminder notifications should be made available to message recipient for the following events: Message received (“you’ve got mail”); Storage capacity nearly exceeded/exceeded (“mailbox nearly full,” “mailbox full”)

- 2 Principles:
    - For transmission from EHR to EHR, data will be transmitted from end to end in total encryption including the envelope and EOHHS/the State will not retain any of the information
    - Web Portal Users will be using a Web mail approach with secure e-mail. There will be storage limits with notifications to providers informing them that they are close to capacity, but it is up to the provider to manage the use of the available space.
- To address the concern of consumers that the State may have access to their health information, the data encryption will be maintained by a separate entity and the State government/EOHHS will not have access.

Question: What happens when a message gets deleted?

Answer: It may be on back-up /Disaster Recovery (DR) but after a certain time it is gone. The HIE is a true pass through –for Phase 1.

Question: What is the consent process? Does Phase 1 adequately reflect Chapter 305 opt-in/opt-out requirements?

Answer: The consent model is the same as it is currently within a practice. Whatever is the current process will remain the same for Phase 1. The Legal/Policy Workgroup is currently addressing this question and will come back with clarification.

No further questions or comments.

Meeting adjoined at 5:00 p.m.

June 18, 2012 PowerPoint Presentation attached.