

Privacy Officers Forum

**The HIPAA COLLOQUIUM
AT HARVARD UNIVERSITY
AUGUST 21, 2002**

**Elliot M. Stone, CEO
Massachusetts Health Data Consortium
www.mahealthdata.org**

Privacy Officers Forum Mission Statement

Encouraged by the Massachusetts Governor's Health Care Task Force Administrative Simplification Workgroup to assist Privacy Officers & their organizations to comply with HIPAA Privacy Regulations by April 14, 2003 via:

- Convening Bi-monthly meetings
- Facilitating consensus on “reasonable & appropriate” implementation of HIPAA Policies, Procedures, Forms and Templates
- Seeking clarifications as a Community from DHHS and state officials

Privacy Officers Forum Mission Statement (con't.)

Educating Privacy Officers through:

- Regular Meetings
 - Panel Discussions and Case Studies
 - Reports from Forum Subgroups and Other Privacy Entities
 - Consortium's Web Site FAQs – www.mahealthdata.org
-
- A Community Resource: encouraging open sharing of work products, policies, and opinions to:
 - Save Time and Speed Compliance
 - Define Community Standards

Privacy Officers Forum

Privacy Officers Forum Co-Chairs:

- [Anne E. Doyle MBA](#), Compliance & Privacy Officer, Tufts Health Plan
- [Karen G. Grant, RHIA](#), Chief Privacy Officer, Partners Healthcare System

Members

- *Payers & Govt (16)*: Beacon Health Strategies, Blue Cross Blue Shield of MA, BMC HealthNet, CIGNA, Delta Dental Plan of MA, Division of Medical Assistance (Medicaid), Executive Office of Health & Human Service, Fallon Healthcare System, Group Insurance Commission, Harvard Pilgrim Health Care, Harvard University Health Services, Health New England, MIT Medical Department, Neighborhood Health Plan, Tufts Health Plan, United HealthCare
- *Providers (17)*: Baystate Health Systems, Boston Medical Center, Cambridge Health Alliance, CareGroup Healthcare System, Caritas Christi, Children's Hospital, East Boston Neighborhood Health Center, Emerson Hospital, Lahey Clinic, Mass. Medical Society, New England Medical Center, Partners HealthCare, Risk Management Foundation, Southcoast Health System, South Shore Hospital, UMass Memorial Health Care, Winchester Hospital
- *IT Partners (9)* : Cap Gemini Ernst & Young, Computer Sciences Corp., Fidelity Employer Services, IDX Systems Corp., Medco Health Solutions, Novell, Inc., OpenReach Inc., Pricewaterhouse Coopers, WebMD

Privacy Officers Forum

Original Topic Priorities*

Discussed:

- ✓ Consents
- ✓ Authorizations
- ✓ Business Associate Contracts
- ✓ Chain of Trust
- ✓ Accreditation Organizations
(JCAHO, NCQA)
- ✓ State Law Preemption
- ✓ Minimum Necessary
- ✓ Research: IRBs
- ✓ Employer/Health Plan Sponsors
- ✓ Training
- ✓ Employers as Covered Entities
- ✓ Notice of Privacy Practices

Upcoming:

- Role Based Needs
- De-Identification
- Verification of Identity
- Final Privacy Rules
- Designated Record Sets
- State Law Pre-emption

*** Survey #1: October 2001**

Privacy Officers Forum

Updated Topic Priorities*

- Definitions of Designated Record Sets
 - Accounting of Disclosures
 - Employer and HIPAA
 - Right to Request Privacy Protection for PHI
 - Policy and Procedure Review/Approval Processes
 - Verification of Identity
 - Role Based Needs
 - Opportunity to Agree or Object to Disclosure
 - Access and Amend PHI
 - Personal Representatives
 - Interface with IT Dept.
 - De-Identification
 - Group Health Plans and Plan Sponsors
 - Uses and Disclosures for Research
 - Marketing
 - Fundraising
- *Survey #2: June 2002 ranking**

Other Suggested Topics*

- State Jurisdiction-by patient residence vs. treatment location
- Budgeting
- Mitigation if breach occurs
- Suggested safeguards when using PHI
- Hybrid entity designation
- Confidential communication
- Patient Rights and requirements

“Ah-Ha” - Lessons Learned: Privacy Officers Forum

A Reasonable & Appropriate Community Approach to Compliance

Professional Judgment: The Rules were NOT designed:

- To put anyone out of Business
- To override the professional judgment of the covered entity
- Providers and insurers can assume that each covered entity is making reasonable judgments when requesting PHI, minimum necessary information...let's not demonize other covered entities

Business Associates: In MOST instances:

- Provider Organizations are NOT Business Associates of the Health Plans
- Brokers are Business Associates of Employers NOT the Health Plans

Pre-Emption: Federal and State Mental Health Law conflicts identified:

- Boston Bar Association will make recommendations to the MA State Legislature

“Ah-Ha” - Lessons Learned: Privacy Officers Forum (con’t.)

Minimum Necessary: An “expanded consciousness” not an adversarial state:

- Can build on “Need to Know” standard, already practiced in many institutions
- Does not require that all risk of incidental use or disclosure be eliminated
- Explicitly provides for use and disclosure that cannot be reasonably prevented, is limited in nature, and that occurs as a by-product of an otherwise permitted use or disclosure
- Some covered entities’ (e.g. providers, health plans, etc.) abilities to implement “role-based access” are currently limited by their “legacy” systems
- All automated applications do not have to be replaced in order to comply
- Some Insurers are considering eliminating “release of info/consent” language from subscriber’s enrollment forms

Reminder: There are many different opinions on how to implement “minimum necessary,” but most would agree, it is more than a presumptive “what-we-currently-do” as the minimum necessary stance - i.e. proclaiming that minimum necessary is nothing but “what I say it is”

“Ah-Ha” - Lessons Learned: Privacy Officers Forum (con't.)

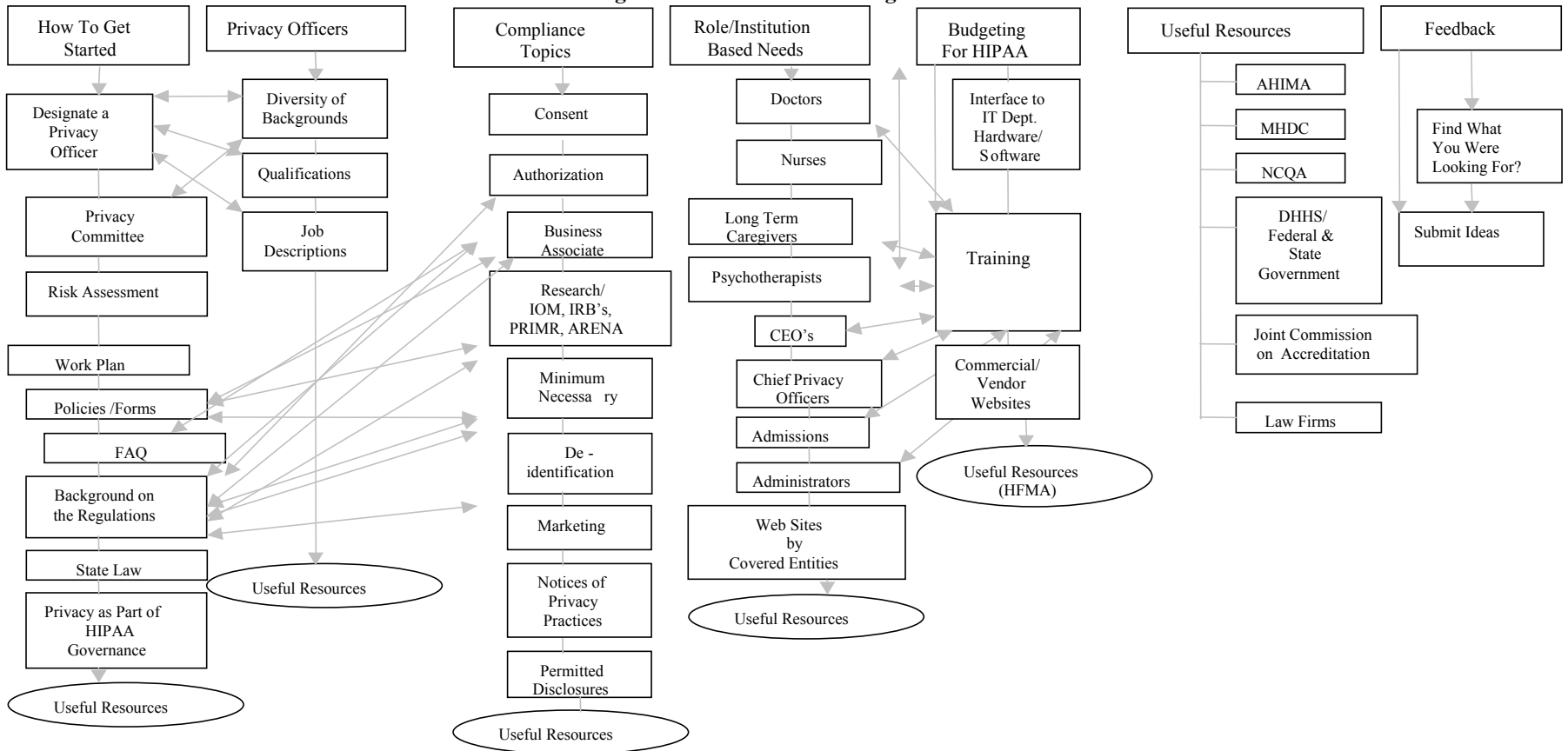
Training: Providers & Insurers are sharing Training Tips!

For example:

- Use actual taped calls (with permission)– case studies work!
- Use real examples of breaches: large & small – case studies
- Explain impact on daily work (optional to mention HIPAA)
- Try to predict which changes will result in improvement
- Make privacy visible (pens, badges, signs etc..)
- Administer pre-training HIPAA surveys
- Internet & CD ROM not accessible to all providers
- Include other compliance messages with HIPAA Privacy Training

Privacy Officers Forum Resources

**Navigation Map: Privacy/HIPAA Sections
Web Site Design: www.mahealthdata.org**



Current Forums

Multiple inter-organizational collaborative bodies

- CIO Forum - focus on inter-organizational health data issues
- Operations Forum - focus on claims process and HIPAA transactions
- HECC - HIPAA Educational Coordinating Committee
- Privacy Officers Forum - focus on HIPAA privacy/compliance
- Security Officers Forum - focus on HIPAA security (kick-off 4/12/02)
- Webmaster Group - quarterly meetings