LAXOR, Inc.

CPS Workgroup

April 12, 2007

John DesMarteau, MD

President & CEO

Privacy & Security

People Are Concerned

- Markle Foundation*
  - 91% of respondents very concerned about privacy & security of health information
  - People with chronic health care issues and frequent health care users somewhat less concerned
- Many recent high-profile data leaks

*2003 Survey of 1,246 US Adults

The Key

- Many PHRs are
  - Not Covered Entities (CE) as ***currently*** defined by HIPAA
  - Should they be?
    - See questions and answers beginning next slide

1) Collection/Sharing of Information

- The LAXOR® PHR is patient-controlled
- To access their PHRs patients must invite their:
  - Providers
  - LAXOR® Personal Health Information Managers (PHIMs)
  - Family Members

1) Collection of Information

- Document Uploading by Patients, Providers & LAXOR® PHIMs
  - Faxes to Digital via LAXOR® Fax-Server
    - LAXOR® Toll-free number
  - Scans to Digital
    - Local: Patient-controlled PCs
    - Remote: PHIM-controlled PCs
  - Native Digital Document
    - Local: Patient-controlled PCs
    - Remote: PHIM-controlled PCs

1) Sharing of Information

- Patients Establish Access
  - Providers
  - PHIMs
  - Family Group Members
- Access
  - Routine
  - Emergency
    - Data subset
- Time delimited
  - Providers always have access to data they created

2) Protection

- Storage
  - Hosting: Tier 1 facility
  - Hacking
    - Strong passwords
    - Managed firewalls
    - Database encryption
  - Loss: co-location
    - Mirroring
- Transmission & Access
  - Encryption: SSL for the entire PHR
  - Automatic time-out logouts
- Identity Theft
  - No storage of SSN or credit card numbers

3) Privacy & Security Breaches

- Notification of Clients
  - Paramount
- Administrative
  - Internal Breach Management
    - Termination
    - Possible criminal charges
  - External Breach Management
    - Business Associate agreements
      - Same standards as LAXOR®
- Physical
  - Repeated threat analysis and threat testing
- Technical
  - Repeated threat analysis and threat testing

4) Communication of Protection

- Notice of Privacy Practices
  - Public Website
    - Summary
    - Downloadable as PDF (Copies available)
  - PHR itself

5) Consumer Control

- The LAXOR® PHR is:
  - Patient-owned
  - Patient-controlled
    - Patients *can* append comments to any document
    - Patients *cannot* change documents provided by their providers
    - Access is granted by the patient

6) Operation of Law

- LAXOR® is not a HIPAA covered entity (CE)
- Yet voluntarily follows HIPAA where appropriate to its business operations

7) LAXOR® Abiding By HIPAA*

- Believes improves competitiveness
  - Increases LAXOR's trustworthiness
- Believes improves interoperability
  - Facilitates data acquisition from data creators
    - Especially health care providing organizations

*Where applicable to LAXOR's business operations

8) HIPAA Compliance

LAXOR®

- Not a Covered Entity as defined by HIPAA
  - Is not a health plan
  - Is not a health clearinghouse
  - Is not a health provider
- Yet abides by HIPAA*
- Does not feel cost outweighs benefits
  - Has done so essentially from inception
  - Improves competitiveness via trustworthiness
  - Improves interoperability

*Where applicable to LAXOR's business operations

9) Minimum HIPAA Privacy Set*

Need to Balance Access/Use with Protection

- Ability to Amend (§164.526)
  - Patient-entered comments into the LAXOR® PHR
- Access & Right of Restriction (§164.524; §164.522)
  - Emergency & Routine
  - Already under LAXOR® members' control
- Business Associates (§164.308; (§164.314)
- Complaint Management (Chief Privacy Officer) (§164.530)
  - Method in place
  - Documentation of complaints
  - Workforce sanctions
  - Mitigation of complaints
  - No retaliation

*As appropriate to LAXOR's business operations

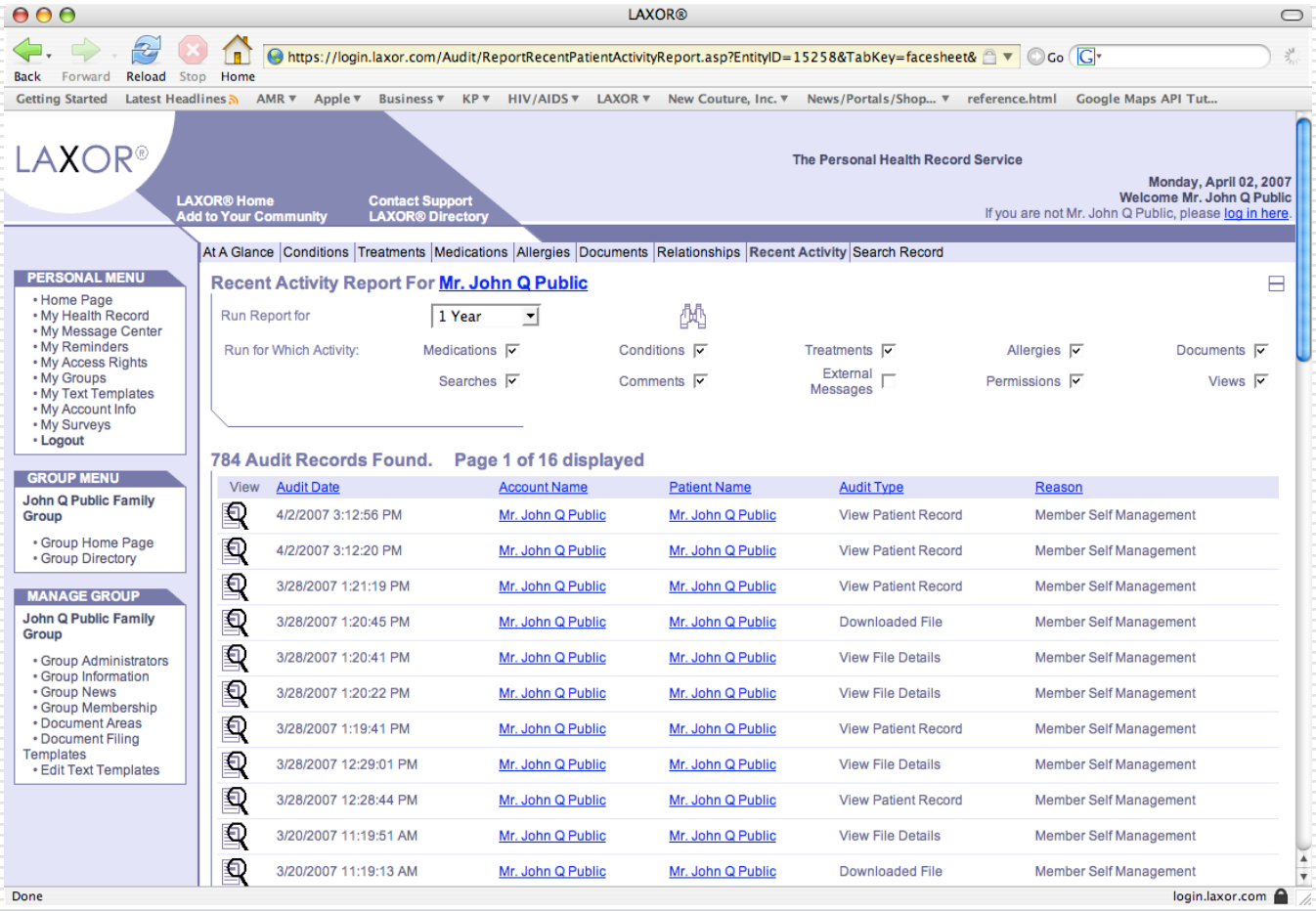
9) Minimum HIPAA Privacy Set*

Need to Balance Access/Use with Protection - Continued

- Disclosure Accounting (§164.528)
  - LAXOR's patient-controlled automatically generated, always available audit trail (see next slide)
- HIPAA Training (§164.530)
- Limited data set & usage for research (§164.514)
- Marketing (§164.508)
  - Opt-in only
  - PHIMs acting as intermediaries - no direct connection with vendors except by patient request
- Minimum Necessary (§164.514)
- Notice of Privacy Practices (§164.520)
- Policies & Procedures (§164.316)

*As appropriate to LAXOR's business operations

9) Example: Disclosure Accounting



10) Non-Relevant HIPAA Principles

- Authorizations (§164.506; §164.508; §164.510)
  - No use of PHI by LAXOR® for treatment, payment or health care operations
    - Acceptance of terms of usage (TOU) conditional to use of LAXOR® PHR
      - Members control access and therefore disclosures for:
        - Emergency access
        - Routine access
- Facility Directories (§164.510)

11) Certification Process

LAXOR® Submission dependent on:

- Requirement specifications
- Cost
  - Time
  - Personnel
- Periodicity
- National acceptance for value
  - Governmental promotion of the certification standard

12) Market Forces

- Competition
  - Marketing advantage
- Consumer Trust
  - Much concern on part of consumers
  - Trustworthiness is vital to usage
- Liability
  - The PHR business is a fledgling industry
    - One major mishap could imperil LAXOR® or even the industry as a whole

13) Business Associates

- LAXOR not yet a business associate, but…
  - Would make certain that its operations meet requirements of any entity for which it becomes a business associate
    - PHR companies that are not health plans, clearinghouses or providers should have a business associate modified to account for the differences in their operations from these entities
  - Business associate agreements negotiated by CEO with assistance of LAXOR's counsel
    - LAXOR will be developing a standard contract appropriate to its business operations for its business associates

13) Business Associates

- LAXOR® has one subcontractor
  - Provides hosting services only
  - Has signed a robust confidentiality agreement
- LAXOR® feels that accountability for meeting ***relevant*** HIPAA requirements is vital to its business operations

Contact Information

John DesMarteau, MD FACA
President & CEO
LAXOR, Inc.
4651 Massachusetts Ave NW
Washington, DC 20016
TF: 866-233-3606 • M: 202-744-4441
John.DesMarteau@laxor.com