Integrating privacy and security in a primary care medical group

Patrick Curran

Physician Resource Northwest, LLC

June 5, 2003

Presentation summary

- Why we did what we did
- What we learned along the way
- What we will do next
- What we would have done differently

Goals for attendees

- Evaluate your plan for security implementation
- Learn how a medieval philosopher can help with HIPAA

Background

- Primary care group with 33 physicians, 7 nurse practitioners, and 175 staff.
- Five clinic sites in Portland metropolitan area
- No written policies for privacy/security existed (circa 2002).
- Culture: state vs. federal control

Oregon HIPAA Forum

- Started in mid-2001
- Representatives from payers, providers, and vendors all participated
- Oregon Medical Association hosted quarterly forums and facilitated sub-committee formation.

Lesson learned: competitors can collaborate.

First cut (early 2002)

- Lacked documentation, but processes were sound.
- Made assumptions:
  - Clinics will resist implementation of too much at one time.
  - Final security rules may cause additional work.
- Conducted first training sessions

Lesson learned: it's not because we have to.

Second cut (mid 2002)

- Too much overlap with privacy existed to avoid addressing security.
- Non-overlapping areas were crucial to ongoing operations.
- We observed an accelerating rate of interest in new devices/access (home users, PDAs, laptops)
- Staff/providers viewed security as an IT issue

Lesson learned: yes, it is because we have to.

Security policy categories

- **Facility security**
- *User identification*
- *External vendors*
- *Granting/modifying access*
- *Workstations*
- **Confidentiality**
- Computer system inventory
- Equipment control
- Data backup
- *Virus protection*
- *Home users*
- System configuration
- Network security training
- Contingency plan
- *Internet*
- Risk analysis

What would William of Ockham do?

- Interpret privacy/security overlap
- Satisfy all constituents
- Implement 40 different policy and procedure categories within compliance dates.
- Educate staff on thousands of pages of rules and guidance

Lesson learned: a liberal arts education actually is useful.

Implementation (early 2003)

- Focused on delivering a compliance program with many elements but only one central theme and one objective.
- Received Board approval and commitment.
- Used interactive quiz format for training.

Lesson learned: make them the expert.

Discussion question examples

- I walk up to the reception area and ask for my free copy of the entire medical record as entitled under HIPAA. I'll wait right here while you copy it, thank you very much.
- A woman calls on the phone checking on the account status for her elderly father. She asks questions about the bill and about the lab test performed that is still not paid by insurance.
- A man arrives at the clinic, introduces himself as the fire marshal, and lets you know he is going to test the fire extinguishers.

Fictitious clinic

IMA is an internal medicine practice with four physicians and twelve employees in a single office location. The office has a PC-based practice management system, performs its own billing, and uses a clearinghouse to transmit 75% of its claims to various payers.

The clinic performs weekly back-ups using standard tapes, but has not conducted a replacement using the back-up tapes, which are kept onsite in the administrator's cubicle. No physician or staff member accesses the computer system from home, but two physicians have PDAs with pharmaceutical information loaded on them and they routinely take those devices out of the office. The administrator, two physicians, and two other staff members have Internet access and e-mail accounts through an Internet Service Provider.

Each person has a user name and password to log in to the network and to the practice management system. However, it is a tight-knit group. The back-office staff knows each other's password to save time, as does the front-office staff so scheduling will run smoothly.

The clinic has existing office policies and procedures, but the clinic manager has not updated them since arriving at the clinic in 2001.

Implementation (mid 2003)

- Compliance program rollout (April 1)
- Privacy notice (April)
- Release of PHI (May)
- Network security and computer term education (June)
- Password management (July)

Lesson learned: HIPAA is a food best digested in small bites.

Contingency Plan example

Group has in place, and revises as needed, a contingency plan to address unexpected events that may destroy PHI stored on computer systems or make it inaccessible for a period of time.

- **Short-term power outage**
- **Long-term power outage**
- **Damage to computer equipment**
- **Preparation**

What we will do next

- Perform monthly “Compliance Focus” in case study format
- Refine security policies based on security rule guidance
- Reinforce the central theme and single objective
- Address encryption
- Conduct disaster simulation
- Integrate security training with computer training

Lesson learned: remember to wear your seatbelt.

A brief history of the seatbelt

- 1930s – Several U.S. physicians equip their own cars with lap belts and begin urging manufacturers to provide them in all new cars.
- 1954 – AMA House of Delegates votes to support installation of lap belts in all automobiles.
- 1959 – New York considers and rejects a bill to require seat belts in new cars sold in the state.
- 1964 – About ½ of states require seat belt anchors in front seats.
- 1975– Sweden requires 3-point seat belt in front and rear and mandates use by persons 15 and older.
- 1984 – Seven of Canada's ten provinces require use of whatever seat belt system is available.
- 1987 – New York becomes first state to require seat belt use on large buses.
- 2003 – Forty-nine states have mandatory seat belt laws. Only nineteen have primary laws, meaning police can stop a vehicle for no seat belt use.

What I would have done differently

- Envision the final product from the outset.
- Not assume that the majority would resist change.
- Formulate policy categories based on staff needs, not compliance officer needs.
- Challenge staff with more case studies.

Lesson learned: substance does not always trump form.

The End

Contact information

Patrick Curran

Physician Resource Northwest, LLC

Phone: (503) 736-2331

E-mail: pcurran@prnwest.com

Website: http://www.prnwest.com