HIPAA Compliance Professional Roundtable: Advanced Issues in HIPAA Compliance

February 5, 2010

PARTNERS HEALTHCARE

FOUNDED BY BRIGHAM AND WOMEN'S HOSPITAL
AND MASSACHUSETTS GENERAL HOSPITAL

Public Confidence in Privacy and Security of Electronic Health Records is Lacking!

Survey 1,000 MD's in Massachusetts

Electronic Health Information Exchange:

- 86% think it would improve care quality
- 76% believe it would save time
- 70% say it would help lower costs
- 71% concerned about privacy breaches:
  - 55% somewhat concerned
  - 16% very concerned

US News Article/JAMIA: January, 2010 17:66-70

Data: *When* you need it and *Where* you need it

Critical for Patient Care/Safety

Known Benefits

Potential Risks

5 Key Areas that need to be Addressed

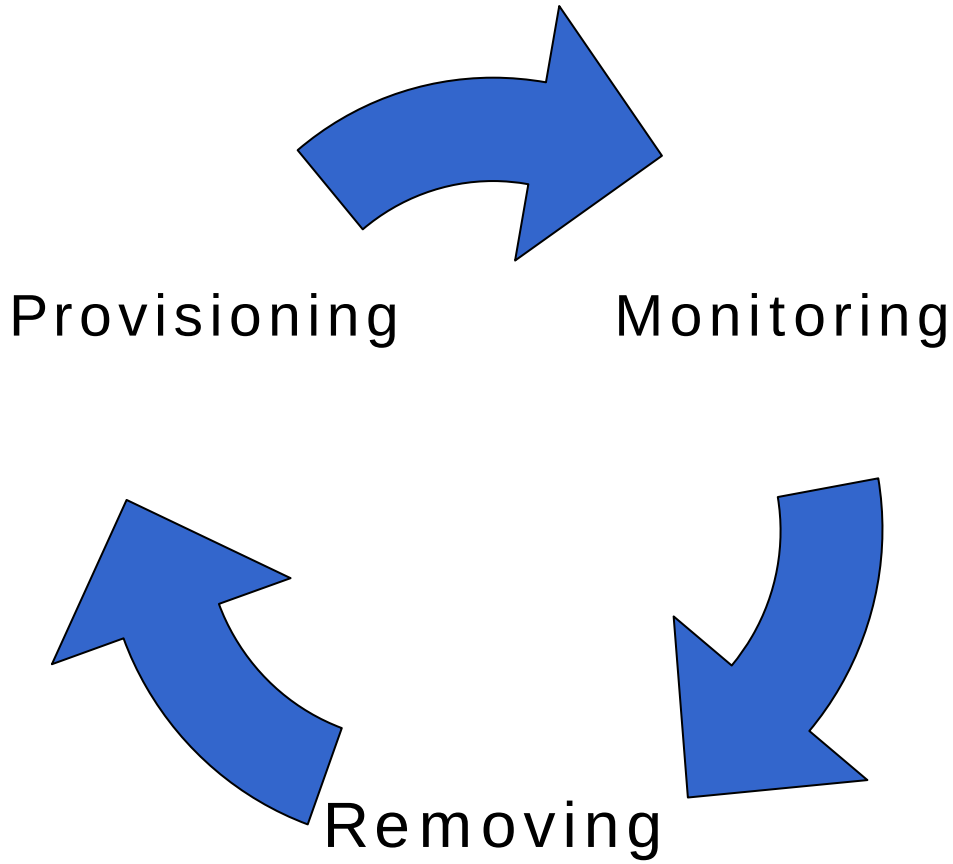
(this list is certainly not all-inclusive!)

- Access Management
- Auditing
- Patient-Centered Data Management
- Safeguarding Portable Devices
- Consent

1. Access Management

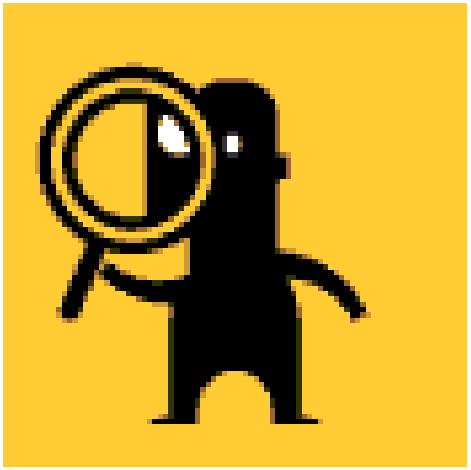
PARTNERS HEALTHCARE | FOUNDED BY BRIGHAM AND WOMEN'S HOSPITAL AND MASSACHUSETTS GENERAL HOSPITAL

- Access should only be permitted for those with a current business need
- Access should be limited to only the systems/applications needed for the intended business purpose



2. Auditing

PARTNERS HEALTHCARE | FOUNDED BY BRIGHAM AND WOMEN'S HOSPITAL AND MASSACHUSETTS GENERAL HOSPITAL



Patient Record Audits

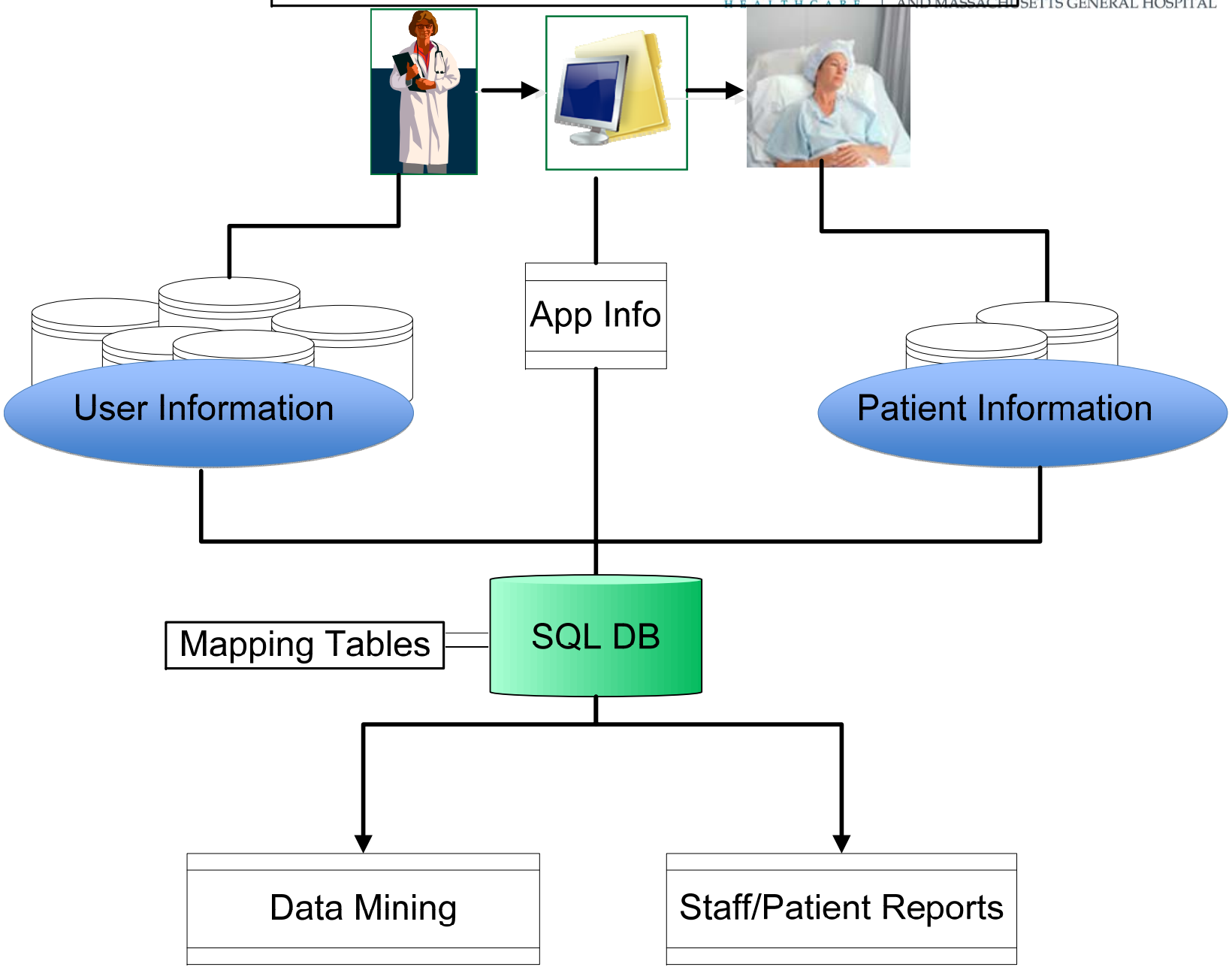
- ✓ Employee Self Audit
- ✓ Manual audits: VIPs
- ✓ Manual audits: complaint-based
- ✓ Manual audits: risk-based

Why not Review All Audit Records to find Privacy Violations?

Monitoring Activity Patterns

- Identification of unusual access patterns:
- If the credit card companies can do this, ***WHY CAN'T WE??***
- We need to better understand:
  - ***Who*** are these Users?
  - ***What*** are they doing?
- Monitor ongoing accesses with near real-time ***context*** information.

Record Access Events



Create a Culture of Awareness

Time now: 12:44

Enhanced Monitoring:
***Who* are you**
and *What* are you doing?

3. Patient-Centered Data Management

PARTNERS HEALTHCARE | FOUNDED BY BRIGHAM AND WOMEN'S HOSPITAL AND MASSACHUSETTS GENERAL HOSPITAL

- Improve Patient Access to Data
  - Accessible, reliable educational materials to support the information available
- Use of Patient Portals for bi-directional communication between providers and patients
  - Patient and provider acceptance
- Should patients be permitted to suppress information in their health records?
  - They do this today by verbally withholding information?
  - Could this negatively impact the provider's confidence in the record?
  - Do patients understand the potential quality of care risks?
  - What is the liability if an adverse event occurs?
  - The better we protect the information up front the less of an issue this will become

4. Safeguarding Portable Devices

- Lost devices containing PHI/PII are costly from a financial and reputational perspective
  - Data breach incidents cost U.S. companies $202 per compromised customer record in 2008, compared to $197 in 2007.
  - the largest cost increase in 2008 concerns lost business created by abnormal churn, meaning turnover of customers.

    PGP Corporation, and the Ponemon Institute, a privacy and information management research firm, fourth annual U.S. Cost of a Data Breach Study, 2/2009.

- Need *to build/restore Consumer Confidence*

5. To Consent or Not to Consent - Considerations?

- The type of information in combination with state and/or federal laws that may impose legal requirements in terms of release of information
- Opt in versus Opt out consent for Electronic Health Exchanges
- Paper, Hybrid, and Electronic Records and Changing Workflows
  - Provider burden
  - Patient Rights
  - Laws need to catch up with the technology
  - Focus on what is meaningful and important to Patients