Data, Monitoring and the Culture of Privacy

Lauren Steinfeld
Chief Privacy Officer

Andrea Thomas-Lloyd
Director, Information Assurance

April 9, 2019

ABOUT PENN MEDICINE

The University of Pennsylvania Health System was created in 1993 and consists of six hospitals (Hospital of the University of Pennsylvania, Presbyterian Medical Center, Pennsylvania Hospital, Chester County Hospital, Lancaster General, and Princeton Healthcare), a faculty practice plan, a primary care provider network, two multi-specialty satellite facilities, home care, hospice and a nursing home.

| Licensed Beds | 2,876 |
| Total Employees | 39,394 |
| IT Operating Budget | $233,866,741 |
| Operating Revenue | $7.8 Billion |
| Adult Admissions | 135,893 |
| Outpatient Visits | 5,410,827 |
| Physicians | 6,818 |

* Includes HUP, PAH, PPMC, CCH, LGH, PMPH, CCA, Corp, CPUP, HCHS
~ Includes HUP, PAH, PPMC, CCH, LGH, PMPH, CCA, Corp, CPUP, HCHS
3 Includes CCA/CHCA
2 Includes physicians with privileges at more than one hospital
The Perelman School of Medicine — established in 1765 — is the nation’s first medical school. It is consistently ranked in the nation’s top academic medical schools by US News & World Report.

<table>
<thead>
<tr>
<th>Faculty &amp; Staff</th>
<th>6,203</th>
</tr>
</thead>
<tbody>
<tr>
<td>State Research Funding</td>
<td>$1.8mil.</td>
</tr>
<tr>
<td>Licensing Revenue</td>
<td>$31mil.</td>
</tr>
<tr>
<td>New Patents Awarded</td>
<td>85</td>
</tr>
<tr>
<td>MD Students</td>
<td>769</td>
</tr>
<tr>
<td>PhD Students</td>
<td>629</td>
</tr>
<tr>
<td>MD/PhD Students</td>
<td>191</td>
</tr>
<tr>
<td>Residents &amp; Fellows</td>
<td>1,331</td>
</tr>
<tr>
<td>Postdoctoral Fellows</td>
<td>731</td>
</tr>
</tbody>
</table>

Total Figures as of FY18

Privacy Program Early Days

- HIPAA Compliance
- Early building blocks:
  - Infrastructure
    - Privacy Office within OACP
    - Entity Privacy Officers
    - Oversight Committee
  - Policies and Procedures
  - “One and done” Training
  - Business Associates identification and contracting
  - Management of Complaints and Incidents
### 2013 HITECH – Breach Notification as Game Changer

- Increasing maturity of program
  - Focus on compliance and risk
  - Focus on all pertinent laws and other sources of requirements

- Breach notification as game changer

- Increase in attention from organizational leadership in healthcare organizations nationwide

- Privacy monitoring gets a higher profile
  - Early stage technology
  - Some proactive use; reactive use

### And now . . . Formalized Privacy Monitoring

- Most transformative development in recent years
- Engaging at every level
- Serves as deterrent and detection tool
- Strengthens and demonstrates organizational commitment

|-------|------|------|-----------------|
Privacy Monitoring – What

- Privacy monitoring is not software; Privacy monitoring is a program
  - Commitment by organization to people, process, and technology to detect and deter inappropriate access to systems
- Privacy monitoring system is nevertheless a critical component of the program
- Dedicated personnel are needed to intake from system and other sources and determine where investigations are warranted
- Investigations must be conducted according to fair and effective procedures, in partnership with appropriate HR and other units
- Organization commits to respond with discipline, mitigation, and messaging

Privacy Monitoring – Why?

- Compliance ➔ HIPAA Security Rule – 45 CFR § 164.308 Administrative Safeguards
- Supporting Strategic Priorities
  - Increased access to PHI means better treatment, care coordination, cost containment, research opportunity, and poses RISK
  - Trend in healthcare – dramatic increase in information sharing:
    - Health information exchanges
    - Clinical system platform programs. Examples: Care Everywhere, EpicCare Link, Community Connect
  - Research enterprise
  - Audits and governmental oversight
- Privacy monitoring as critical control supporting this additional sharing
Privacy Monitoring – How? Technology

- Artificial Intelligence identifies anomalous user behavior across systems
- Easily integrate disparate information system logs and data
- Ability and flexibility to prioritize areas of focus
- Contextual awareness from outside sources – social media, major news sources
- In depth, automated case analysis
- Tailorable Areas of Focus
  - Suspicious Access
  - Co-worker
  - VIP
  - Neighbor
  - Family

Privacy Monitoring – How? Technology

- Gearing up
  - Understanding the technology
  - Permissions to use data
  - Contracting
  - Security review
- Data feeds
- Testing
- Policy questions:
  - Will we allow access to own record?
  - Will we allow authorized access for family and friends?
  - What are the priority concerns?
  - How should we message to community?
  - How will we measure success?
Privacy Monitoring – How? People and Process

- Investigators, Human Resources, Practice and Department Leadership and more
  - No playbook
  - Training and awareness
  - Roles and responsibilities
  - Relationship building – Win/win allies

- Investigation SOPs
  - Exhaust all non-human intervention first
  - Coordination with HR, contacting supervisors, interviewing individuals
    - Order of communications
    - Rules of the road – 2 interviewers; HR always present
  - Sanctions Guidance – recommendations and decisions
  - Mitigation and Lessons Learned
  - Breach reporting

Privacy Monitoring – How? Messaging to Community

A balancing act: seriousness of patient privacy versus sense of big brother

- This is real
- Do not be surprised
- We are watching
- No interest in “gotcha”
- No one loses their job over a database report
- Human-led investigations with great sensitivity
- Do not let this program stop you from doing your job
Leadership Reporting

- Leadership must be prepared for impact of Program
  - Sea change
  - Commitment to process
  - There will be controversy

- Use of program data and trending for periodic reporting
  - Incident documentation review/reconciliation
  - Dashboard development

- Key metrics tracked:
  - Violations
  - Breaches
  - Corrective Actions
  - Training compliance

Lessons Learned

- Impact:
  - Possibly most transformative initiative to create a culture of privacy
    - Even where no violation; questions being asked has a big effect
  - Engagement at every level
  - Cements partnership with HR, managers, and leadership
  - One kind of privacy problem, with all the right ripple effects

- Do not underestimate resource commitment

- Continuous learning . . .