The New Generation of Privacy Programs
Putting “privacy by design” into practice in complex multi-partner medical settings

Susanna Partrick
Debora Marsden
Jennifer Archie
Debora Marsden
Compliance and Privacy Officer
NewYork Presbyterian Hospital
New York, New York

Susanna Partrick
Senior Privacy and Compliance Administrator
Weill Cornell Medical College
New York, New York

Jennifer Archie
Partner
Latham and Watkins
Washington, D.C.
What does “privacy by design” mean in the context of complex, multi-partner healthcare environments?

How can data sharing partners “build in” privacy to their business processes, especially in an era of Big Data and innovation?

How is privacy considered before, at the start of, and throughout the development and implementation of initiatives that involve the collection and handling patient information?

What are practical ways you can mature and optimize data sharing and governance practices in a multi-institution environment?

We also will review pertinent lessons from recent OCR enforcement under the federal Privacy rule.
Engineer privacy directly into the design of new initiatives as a core consideration

Compliance with regulatory frameworks is the starting but not ending point in decision-making

Privacy considerations are proactively introduced at the ground floor of new projects and initiatives, not bolted or added on later

Privacy is a shared commitment by stakeholders

Projects are monitored to assure that stated promises and objectives related to patient data are being met
Getting started

- Executive leadership sets tone and policy (similarity of approach, outlook and priorities)
- Tools and checklists to ensure that everyone is following similar steps
- Embedded privacy expertise via training and consultation of Chief Privacy Officers
- Staff education
What does that mean for health care at the project level?

- **MAP.** How is personal data collected, used, shared, discarded, secured in the new system or process?
- **RISK ASSESS.** What are the operational risks to privacy, that might result from inadequate or failed internal processes and systems, external events, staff issues, service providers or other third parties?
- **MINIMIZE.** Is there a specific and compelling purpose for the scope of personal data that is contemplated?
- **DOCUMENT.** Develop specific privacy requirements (i.e., user access controls), and test and confirm them.
- **TRAIN.** Participants should understand the purposes of the collection/use case, whether sharing is occurring, whether consent is required, how to process requests for access, referring complaints
- **MONITOR.** Check back, ask questions
- **OPTIMIZE.** Continuous improvement
Privacy Impact Assessments

- Map the information flow
- Identify privacy risks
- Develop an approach to manage the risks
- Multi-stakeholder process
- Living documents
Real World Scenarios
Case Study

* Full-time Faculty Physician of AMC-A who has privileges at Hospital B.

* Physician reports that he downloaded patient medical record data onto University issued device which was later stolen/lost.

Which organization owns the investigation?
Which organization manages the breach risk assessment?
Which organization is responsible for imposing sanctions?
Case Study

* Resident employed by Hospital in training in a specialty department at AMC-B, under the supervision of a full-time faculty member of AMC-B who has a dual appointment in AMC-A.

* Faculty member oversees research project of resident that includes data from patient records from Hospital, AMC-A and AMC-B.

* After presentation of research work at specialty society meeting, slides are posted on specialty society website. Columns in chart on one slide become unhidden revealing PHI.

___________________

Which organization owns the investigation?
Which organization manages the breach risk assessment?
Which organization is responsible for imposing sanctions?
Best Practices

- Ability to respond quickly and involve necessary parties
- As a result of prior training, offenders immediately understood impact of incident
- Collaborative mitigation/corrective action
LESSONS FROM ENFORCEMENT
OCR priorities and lessons

* Incidents:
  * Encryption (!)
  * Discarding paper records, old equipment
  * Controls (i.e., unauthorized access to celebrity records)
  * Careless handling of data
  * Press statements

* Outcomes:
  * Was there a mature PIA/training/sanctions program in place pre-Incident?
Program Maturity

- Notices to patients are accurate, comprehensive and prominently displayed including in context
- Institutional ability to perform privacy assessment and risk management in a predictable fashion
- Complaints / violations are handled, and controls are optimized to reflect experience
- Employee training is relevant, role-based, embedded
- Periodic objective reviews (auditing, random reviews, technology tools)
QUESTIONS?