Clinical Research and HIPAA/HITECH in Practice

Soumitra Sengupta, PhD

Associate Clinical Professor
Department of Biomedical Informatics, Columbia University
Information Security Officer, NewYork-Presbyterian Hospital
Information Security Officer, Columbia University Medical Center
Controls on research

• Applicable controls
  – IRB
  – Conflicts of Interest, Efforts Reporting
  – Safety
  – 21 CFR Part 11
  – HIPAA/HITECH

• Some checks are centralized

• Research computing in academic medical centers is mostly de-centralized
De-centralized computing

• What does it mean to the researcher?
  – Flexible technology choices
  – Cost control: Low costs, long use
  – de facto standard technology: Access, Spreadsheet, Email
  – Quick productivity
  – Easy to help each other/collaborate
  – Incremental costs of sophistication
De-centralized computing

• What does it mean to Security Office
  – Large number of computers
  – Replicated clinical/sensitive data, unknown content
  – Unclear ownership
  – Fragmented (too much and too little) system administration
  – Uneven security controls
  – Mixed environments
De-centralized computing

• Historic in nature, reflects the funding model

• Issues with central research computing?
  – Limited flexibility
  – High cost investment
  – Possibility of slow service delivery
  – Not a prevalent model

• Big researchers or departments have better controls, smaller ones typically do not
HITECH Breach notification is forcing...

In last 2 years ...

• Central checks and attestations are going up
  – Costs are significant
• In-depth scrutiny, concurrent with IRB, and more
  – Privacy board, and now, Security board equivalent
• Stricter security standards on PHI systems
  – How strict is strict enough?
• Reluctant data release
  – How do we trust a single researcher?
• Non-standard attestation demand from sponsors
  – The same from us to the sub-contractors

... it is a shock therapy!
Issues with the law & its implementation

• Seems detrimental to adoption of new technology
  – Mobility
  – Cloud

limiting, research flexibility, and perhaps even better controls

• Breach notification is not really linked to harm potential of loss

• OCR audits are only now creating clarity on standards
  – Only now we know one-way Hashing with secret salt is OK for de-identification – and this is significant

• OCR fines have preceded audits, which is unfortunate
A few observations

• Need a serious debate on how not to discourage adoption of new technology in the name of privacy and security
  – What’s really wrong with the controlled use of Google Docs or Dropbox?

• Achieving better privacy and security will be easier through technology instead of process or program forced by fear of punitive action
  – Health care or Research do not drive information technology vendors. Simple, cheap encryption on workstations is available only now from major OS vendors
A few observations

• Participation of academic medical center research professionals in HIPAA was missed, unfortunately relegating research to be not included in TPO
  – Laws would be more balanced as current OCR guidance are proving

• Health care computing is not a nimble entity, and it has tremendous challenges in near future. Research needs to find its proper place in the change so that it is not short-changed.
  – Expecting changes in 21 CFR Part 11 to be stricter and a punitive approach will hurt; allocate time for research to adjust.
Final views

• Big gains are being made in making data more private and secure
• There is no zero risk system, there is no zero cost control
• Have the right constituencies to develop policy
• Clinical research as a profession is about innovation and but also needs the flexibility of a small business to experiment and thrive
• Punitive privacy and security compliance throttle innovation