Data Management Planning for JHU SOM IRB Approval

David Thiemann, MD (dthiema1@jhmi.edu)
Medical Director, Center for Clinical Data Analysis
JHU SOM IRB Data Management Consultant/Reviewer
Associate Professor,
Cardiology, Epidemiology and Health Sciences Informatics
14 July 2017

IRB Data Review Types/Triggers

- IRB Data Consultant
  - Content review
  - >=500 patients OR high-risk data
- JHU Legal Counsel/ Privacy Office
  - Liability/compliance issues-rare
  - De-ID, external sharing
- Information Security
  - Technical review-rare
  - Web apps, cloud apps, externally facing DB
- JHM Data Trust Research Sub-Council
  - Stuart Ray, Chris Chute
  - Policy review-rare
  - External data sharing, conflict of interest

The Basics

- Store raw data/PHI on
  - Enterprise storage (SAFE, REDCap)
  - Study-specific folder on JHED/AD-enabled managed server
  - JHBox (discouraged)
- No PHI on desktops, laptops, thumb drives, CDs
- Separate raw-data and (de-identified) analytic files
- No unencrypted data transmission (email)
- No external data sharing w/o specific permission
- No non-JHM tools (DropBox, Gmail)

IRB Data Management Documents: Plan, Data Security Profile, Data Dictionary

- Plan: 1-3 paragraphs
  - Specifics, not a statement of good intentions
  - Describe data methods/flow, not just storage
  - Explain case finding, data sources
- Either Data Security Profile (simple projects) or Checklist (complex)
- Data Dictionary—list what will be collected

Common Mistakes

- Excel
  - Portable, unauditable, no data typing
- Shared pswd/access
- Using MRN as 1o key
- No data dictionary
  - "We're going to abstract some charts"
- Back-channel/illicit data access
- Absurd data de-ID methods/promises
  - No DIY de-ID for export
- Sample size fibs
  - 498 patients of 5,000
- Unrealistic EMR/Epic expectations
  - Sipping from a dirty fire hose

Non-Epic Registries: New Data Trust Policy/Standards Coming Soon

- Def: Ongoing enrollment, >500 pts
- Excludes
  - Registries required by law/regulation, operational systems, consented clinical trials, external registries
- Technical requirements:
  - MS SQL Server at MTW, designated DBA, logging, monitoring by IT@JH security team
  - JHED/AD authentication, MFA
  - No unnecessary PHI: SSN, address, phone, email
  - No self-service access. No umbrella IRB approval.

Useful URLs

- IRB Data Security Profile form (studies involving >=500 patients): http://www.hopkinsmedicine.org/institutional_review_board/forms/DataSecurityProfile.doc
- IRB Data Security Checklist form (for studies that do not comply with or meet the requirements of the Data Security Profile):
- http://www.hopkinsmedicine.org/institutional_review_board/forms/Data_Security_Checklist.doc
- JHM Privacy Office Use of Data Agreement (for data extracts from JHM enterprise databases, such as Epic, EPR2020, SCM and CaseMix):
- http://intranet.insidehopkinsmedicine.org/privacy_office/_docs/additional_information/Use%20of%20Data%20Agreement_012816_clean.pdf
- JHM encryption standards: http://www.it.johnshopkins.edu/restricted/standards/EncryptedStandardsRevisedAPPROVED030116.pdf