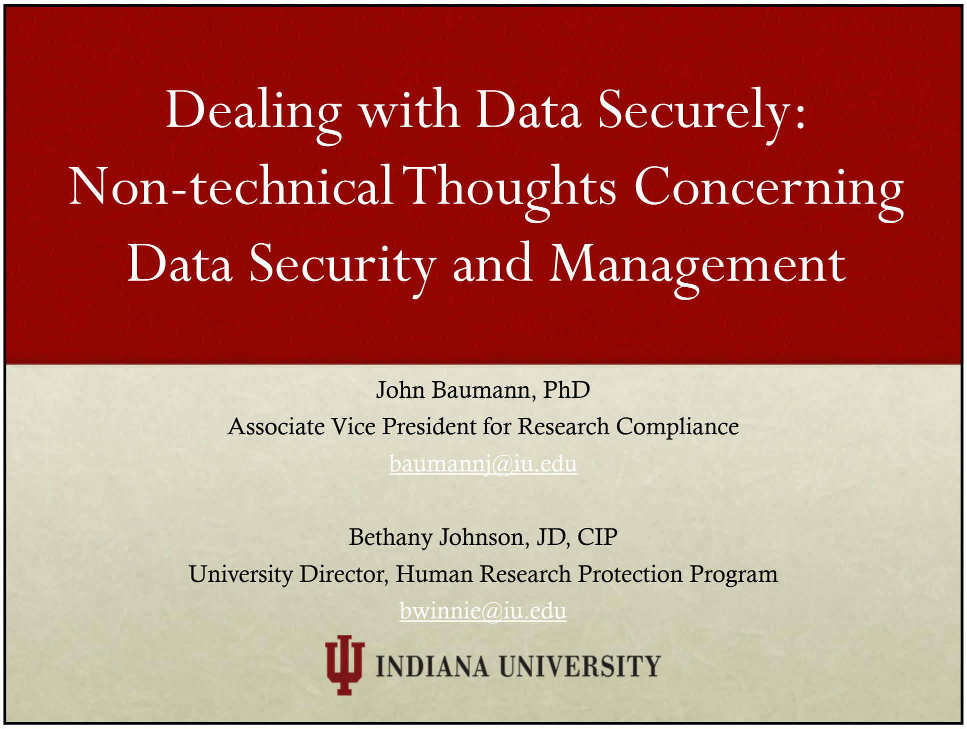


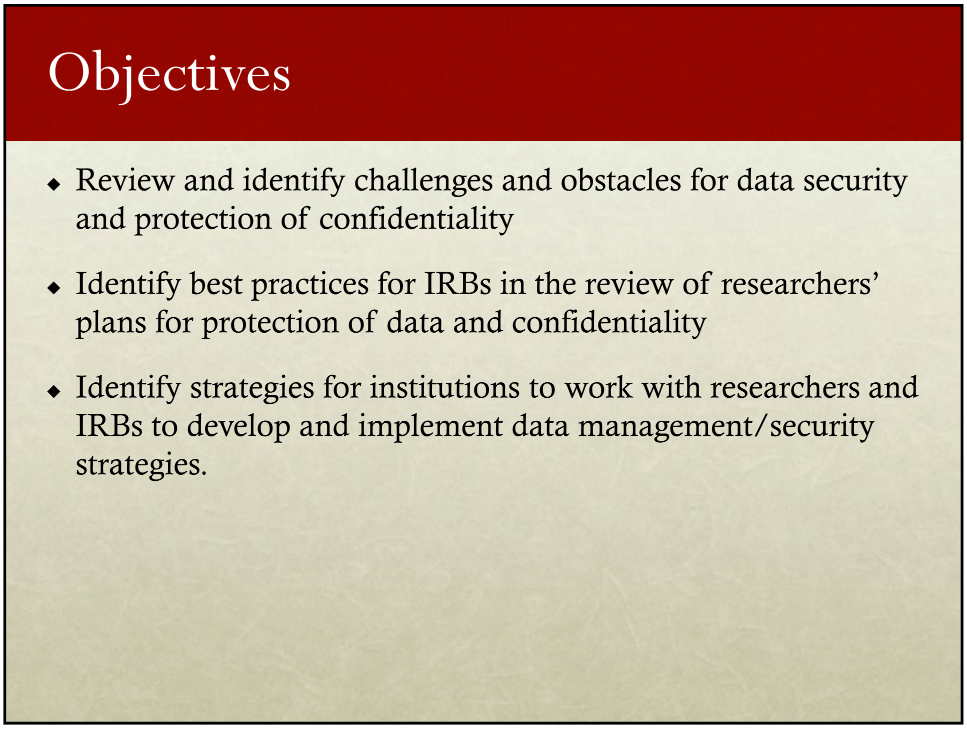
Dealing with Data Securely: Non-technical Thoughts Concerning Data Security and Management

John Baumann, PhD
Associate Vice President for Research Compliance
baumannj@iu.edu

Bethany Johnson, JD, CIP
University Director, Human Research Protection Program
bwinnie@iu.edu

INDIANA UNIVERSITY

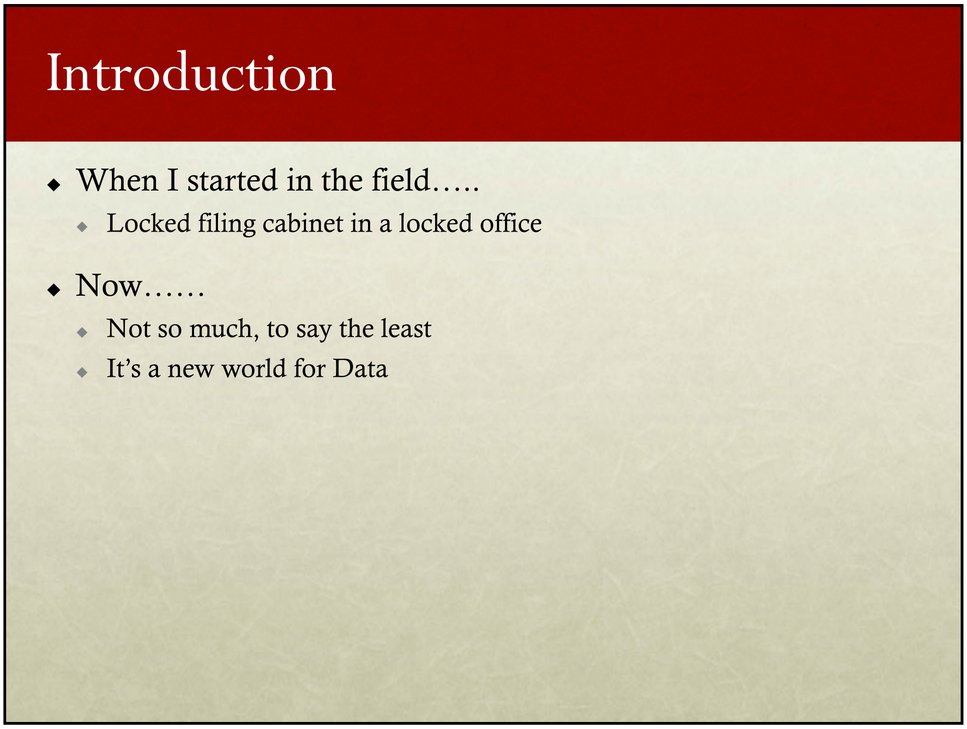
1



Objectives

- Review and identify challenges and obstacles for data security and protection of confidentiality
- Identify best practices for IRBs in the review of researchers' plans for protection of data and confidentiality
- Identify strategies for institutions to work with researchers and IRBs to develop and implement data management/security strategies.

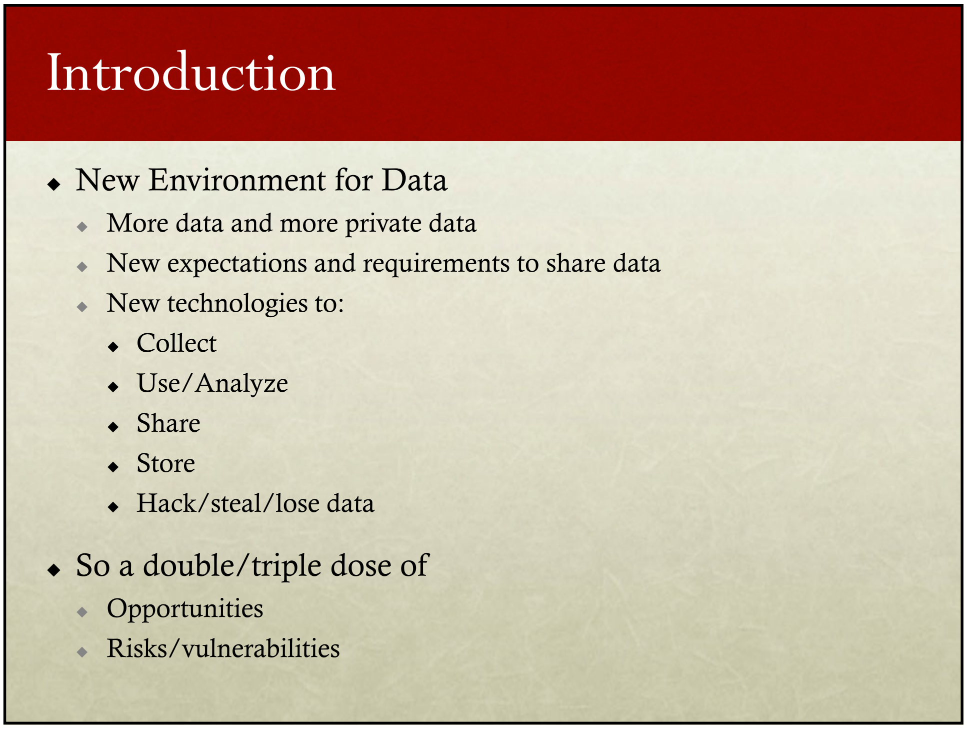
2



Introduction

- When I started in the field…..
  - Locked filing cabinet in a locked office
- Now……
  - Not so much, to say the least
  - It's a new world for Data

3



Introduction

- New Environment for Data
  - More data and more private data
  - New expectations and requirements to share data
  - New technologies to:
    - Collect
    - Use/Analyze
    - Share
    - Store
    - Hack/steal/lose data
- So a double/triple dose of
  - Opportunities
  - Risks/vulnerabilities

4

Introduction

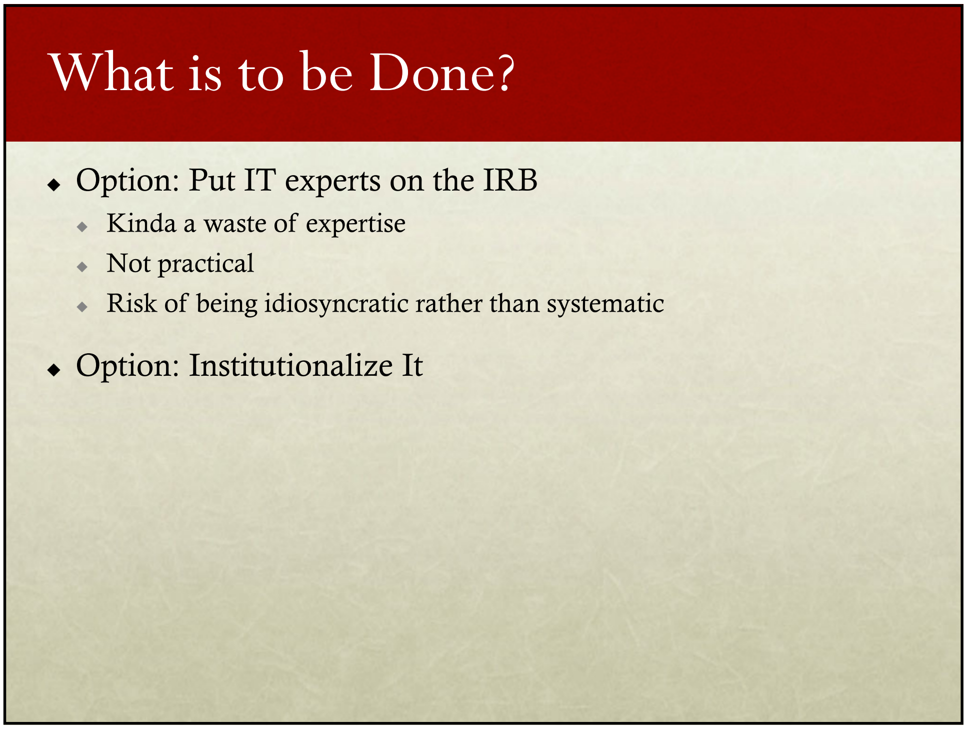
- So….. What is
  - An IRB to do to be prepared?
  - A HRPP to do to be prepared?
  - An Institution to do to be prepared?
- Think in terms of
  - Expertise
  - Technology
  - Requirements

5

What is to be Done? Avoid This

HEY, ROCK BEATS PAPER BECAUSE IT'S HARDER!
NO, PAPER BEATS THE SCISSORS, YOU FOOL!
I GOT A PAPER CUT FROM SCISSORS ONCE...
WHAT ABOUT A STAPLER? DOESN'T THIS BEAT PAPER?
Mayne
WHAT REALLY HAPPENS AT IRB MEETINGS...

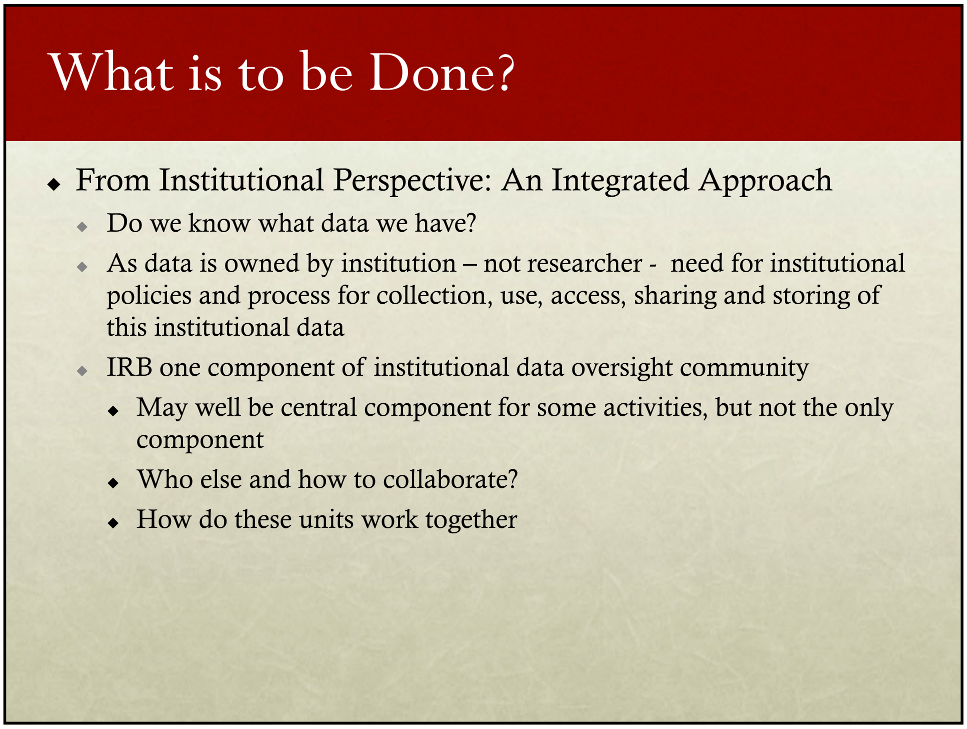
6



What is to be Done?

- Option: Put IT experts on the IRB
  - Kinda a waste of expertise
  - Not practical
  - Risk of being idiosyncratic rather than systematic
- Option: Institutionalize It

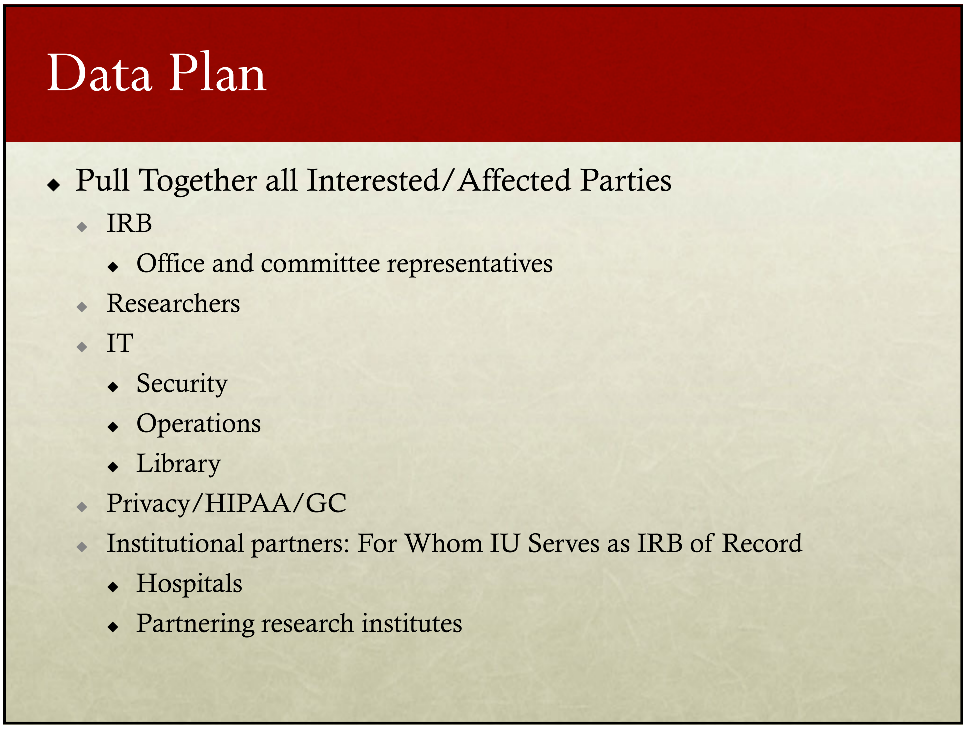
7



What is to be Done?

- From Institutional Perspective: An Integrated Approach
  - Do we know what data we have?
  - As data is owned by institution – not researcher - need for institutional policies and process for collection, use, access, sharing and storing of this institutional data
  - IRB one component of institutional data oversight community
    - May well be central component for some activities, but not the only component
    - Who else and how to collaborate?
    - How do these units work together

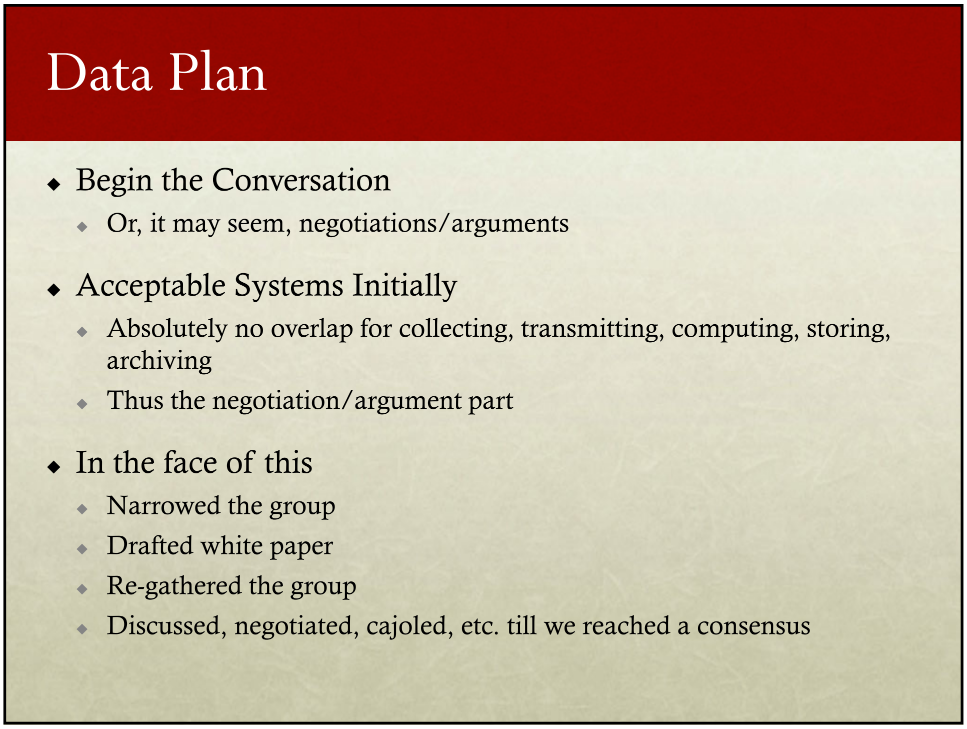
8



Data Plan

- Pull Together all Interested/Affected Parties
  - IRB
    - Office and committee representatives
  - Researchers
  - IT
    - Security
    - Operations
    - Library
  - Privacy/HIPAA/GC
  - Institutional partners: For Whom IU Serves as IRB of Record
    - Hospitals
    - Partnering research institutes

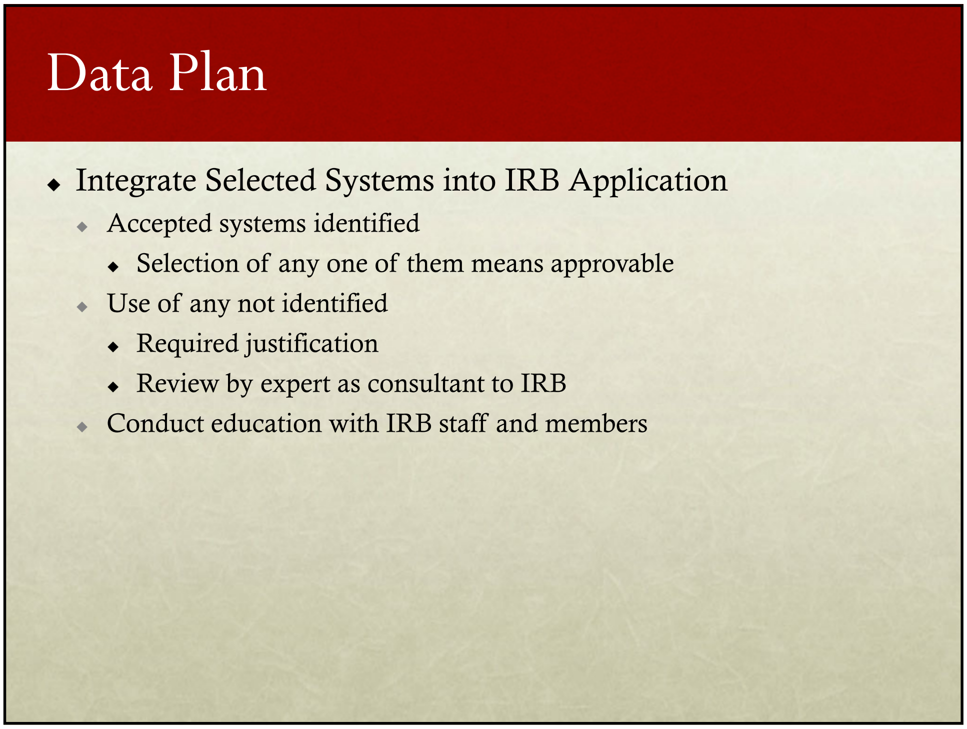
9



Data Plan

- Begin the Conversation
  - Or, it may seem, negotiations/arguments
- Acceptable Systems Initially
  - Absolutely no overlap for collecting, transmitting, computing, storing, archiving
  - Thus the negotiation/argument part
- In the face of this
  - Narrowed the group
  - Drafted white paper
  - Re-gathered the group
  - Discussed, negotiated, cajoled, etc. till we reached a consensus

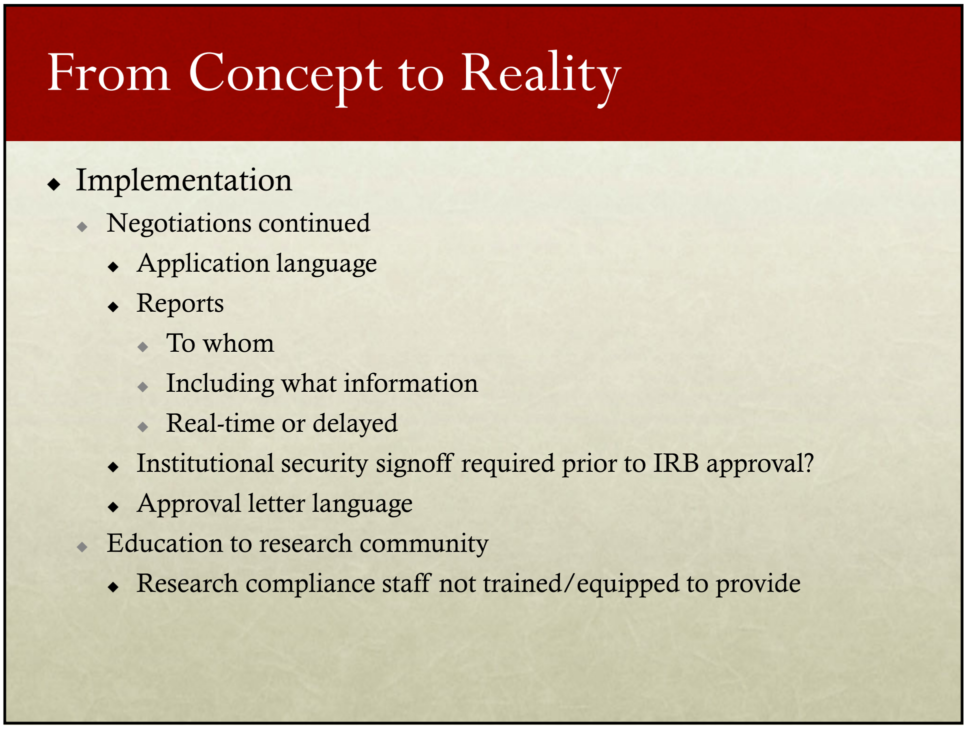
10



Data Plan

- Integrate Selected Systems into IRB Application
  - Accepted systems identified
    - Selection of any one of them means approvable
  - Use of any not identified
    - Required justification
    - Review by expert as consultant to IRB
  - Conduct education with IRB staff and members

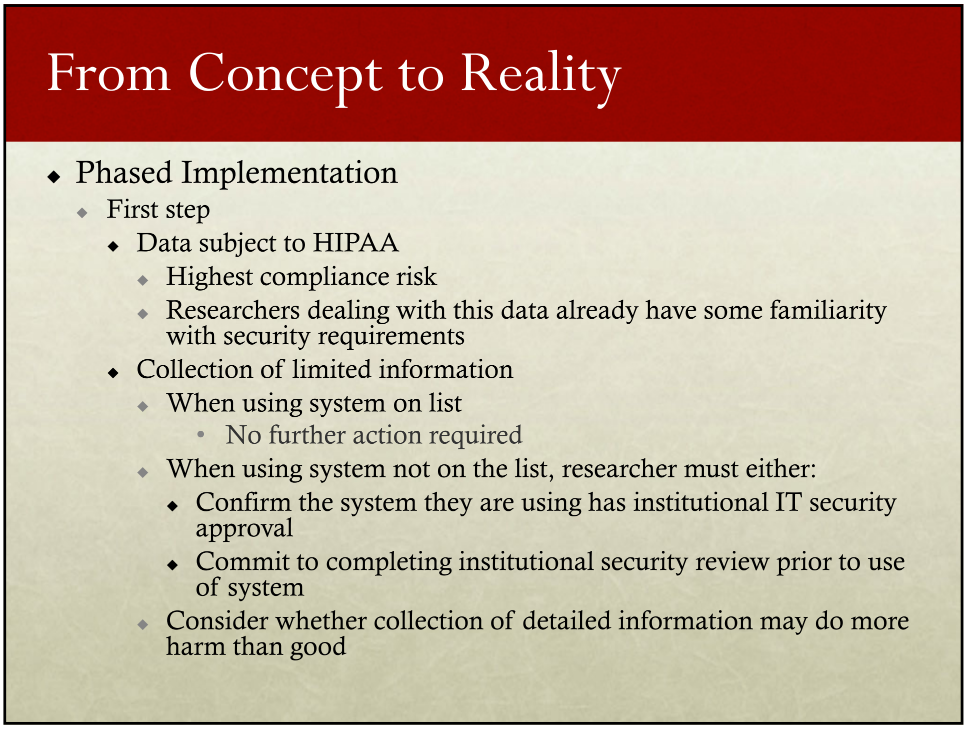
11



From Concept to Reality

- Implementation
  - Negotiations continued
    - Application language
    - Reports
      - To whom
      - Including what information
      - Real-time or delayed
    - Institutional security signoff required prior to IRB approval?
    - Approval letter language
  - Education to research community
    - Research compliance staff not trained/equipped to provide

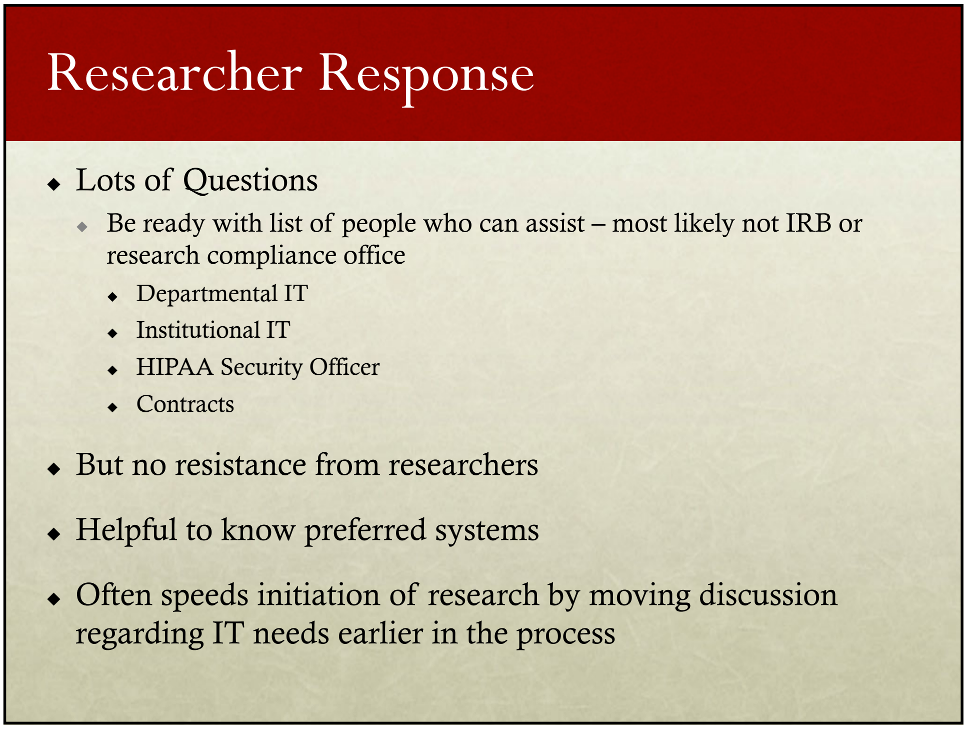
12



From Concept to Reality

- Phased Implementation
  - First step
    - Data subject to HIPAA
      - Highest compliance risk
      - Researchers dealing with this data already have some familiarity with security requirements
    - Collection of limited information
      - When using system on list
        - No further action required
      - When using system not on the list, researcher must either:
        - Confirm the system they are using has institutional IT security approval
        - Commit to completing institutional security review prior to use of system
      - Consider whether collection of detailed information may do more harm than good

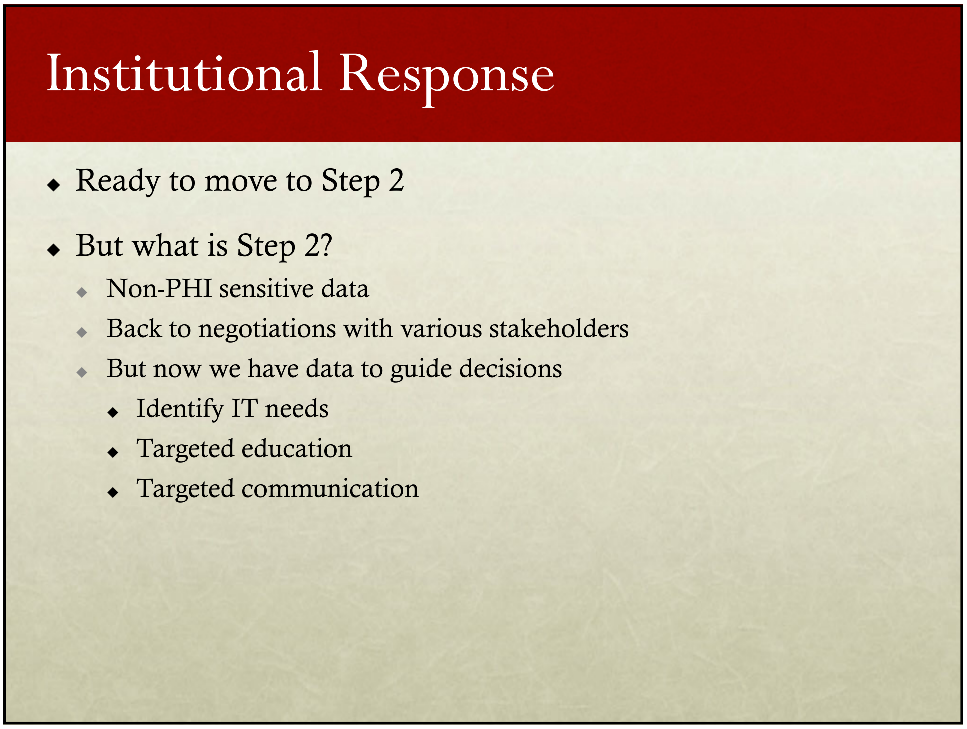
13



Researcher Response

- Lots of Questions
  - Be ready with list of people who can assist – most likely not IRB or research compliance office
    - Departmental IT
    - Institutional IT
    - HIPAA Security Officer
    - Contracts
- But no resistance from researchers
- Helpful to know preferred systems
- Often speeds initiation of research by moving discussion regarding IT needs earlier in the process

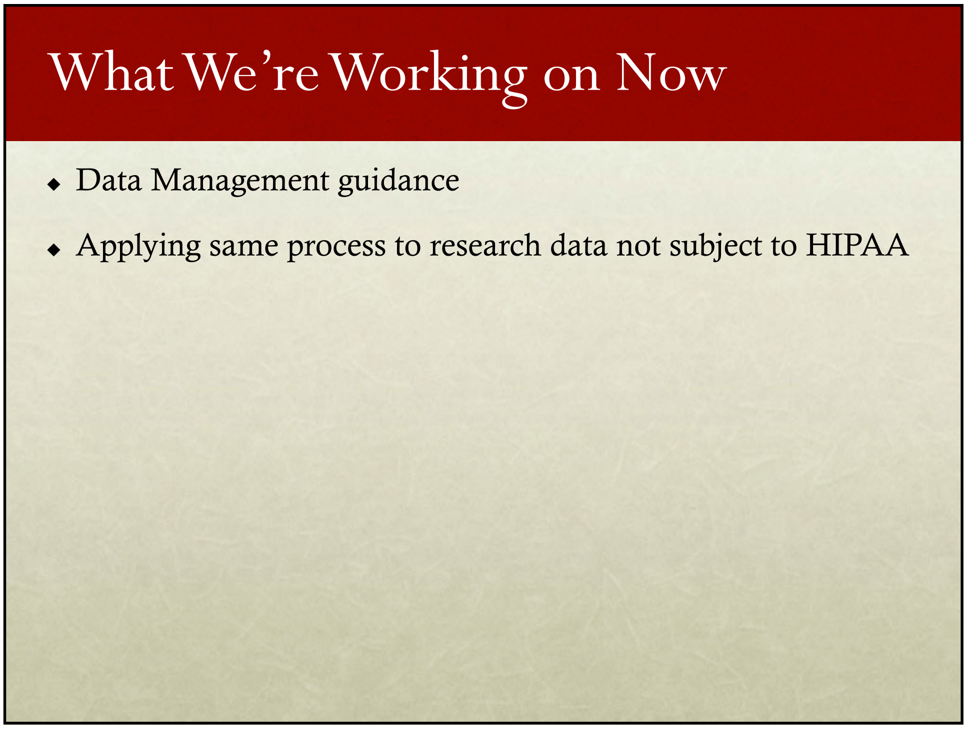
14



Institutional Response

- Ready to move to Step 2
- But what is Step 2?
  - Non-PHI sensitive data
  - Back to negotiations with various stakeholders
  - But now we have data to guide decisions
    - Identify IT needs
    - Targeted education
    - Targeted communication

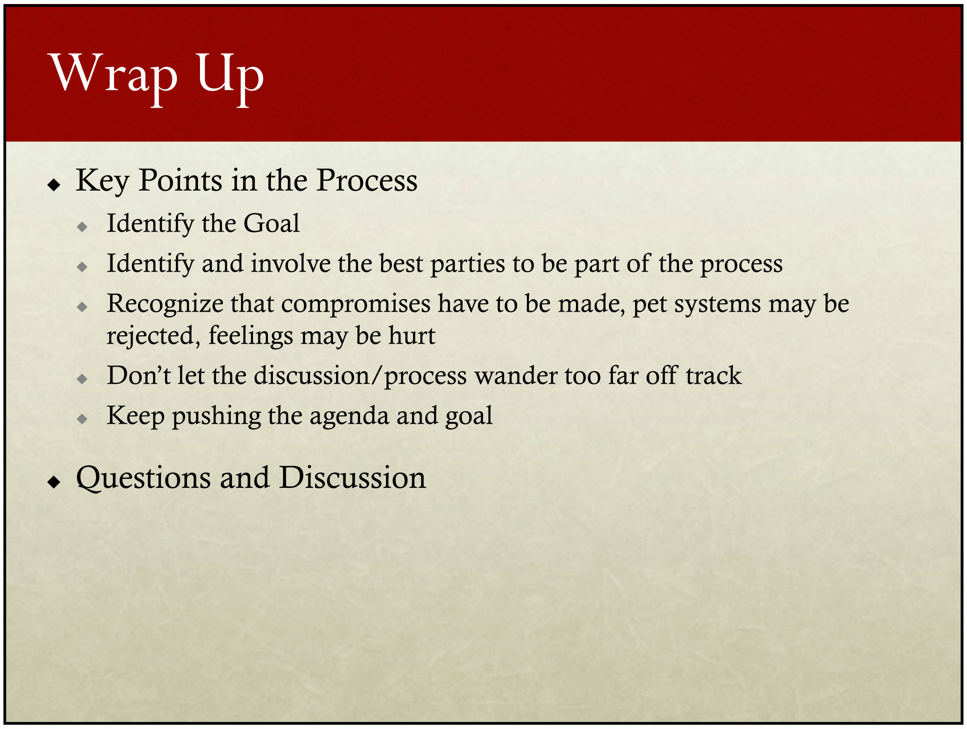
15



What We're Working on Now

- Data Management guidance
- Applying same process to research data not subject to HIPAA

16



Wrap Up

- Key Points in the Process
  - Identify the Goal
  - Identify and involve the best parties to be part of the process
  - Recognize that compromises have to be made, pet systems may be rejected, feelings may be hurt
  - Don’t let the discussion/process wander too far off track
  - Keep pushing the agenda and goal
- Questions and Discussion

17