First Question – Whose Risk is it anyway?
- a roundtable discussion

Use of images from internet – no copyright infringement intended.

June 2019

Shelly Epps, DH Information Security Office

Susan Hayden, DH Office of Research Contracts

Dennis Schmidt, UNC Security, Privacy and Identity Management

B u c k e t, S c o p e, T e m p l a t e, C e n t r a l i z e, A u t o m a t e, T r a i n . . . R e p e a t !

Technology Developer/Owners
Staff/SMEs
Students
Commercial
Research Sponsors
Free/Open Source

Challenges
Conflict of Interest
Varying levels of SDLC expertise
Varying experience in AMC environment
Transitory – ownership issues
Imperfect funnels – low transparency

Technology Targets
Clinical Patients
Research Participants
Staff
Students

Challenges
Different Regs for each group
Different authorization pathways
BYOD
Conflict of Interest

Departments with input
Security, Privacy, Compliance,
Contracts/Procurement/Legal,
Conflict of Interest, Regulatory,
Clinical Governance, IT…..

Challenges
Isolated pillars of review
Duplicated efforts & documentation
Finite review resources
Inconsistency & Churn

Scope out what you can….

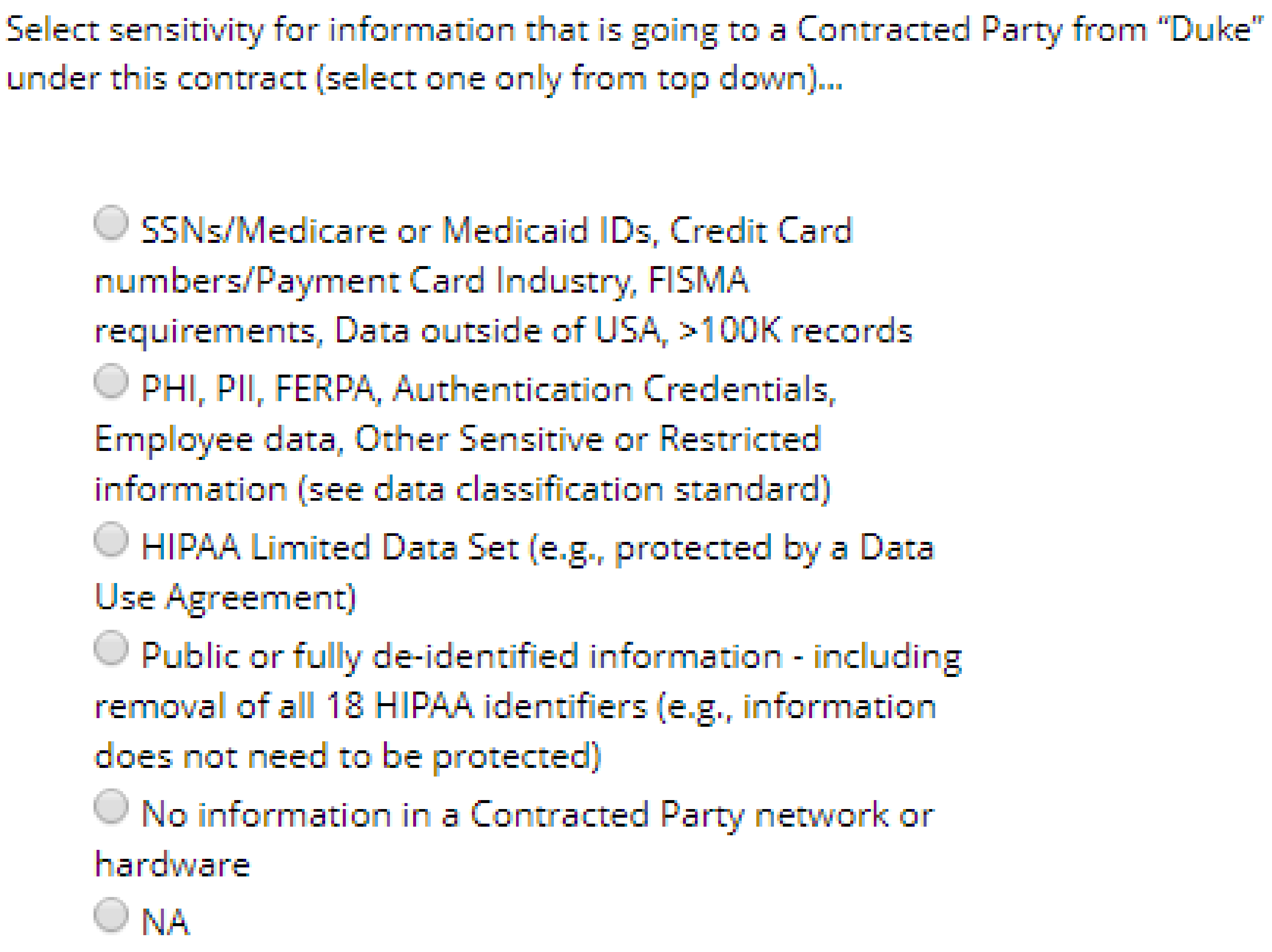
- Risk is everywhere, but not all of it is your responsibility to address.
  - Research sponsors
  - NIH subawards to other entities
  - Commercially available apps
  - ???
- But some of it clearly is your responsibility to address
  - Tech developed by your institution (or on behalf of your instution
  - Branded by your institution
  - Has the potential to impact your network
  - ???

Authorization – put it in your toolbox and develop templates when possible

- Old Language: “except when required by law, no identifying information will be released….”
- New Language: “all research comes with some risk to privacy….”

- Mobile app language
- Unencrypted communication language
- Sponsor contract language

- Find ways to funnel information into centralized pathways that allow for decreased redundancy.
- Automate output when possible
- Maximize your efforts across the highest risk and worst impact.



Select sensitivity for information that is going to a Contracted Party from "Duke" under this contract (select one only from top down)...

○ SSNs/Medicare or Medicaid IDs, Credit Card numbers/Payment Card Industry, FISMA requirements, Data outside of USA, >100K records

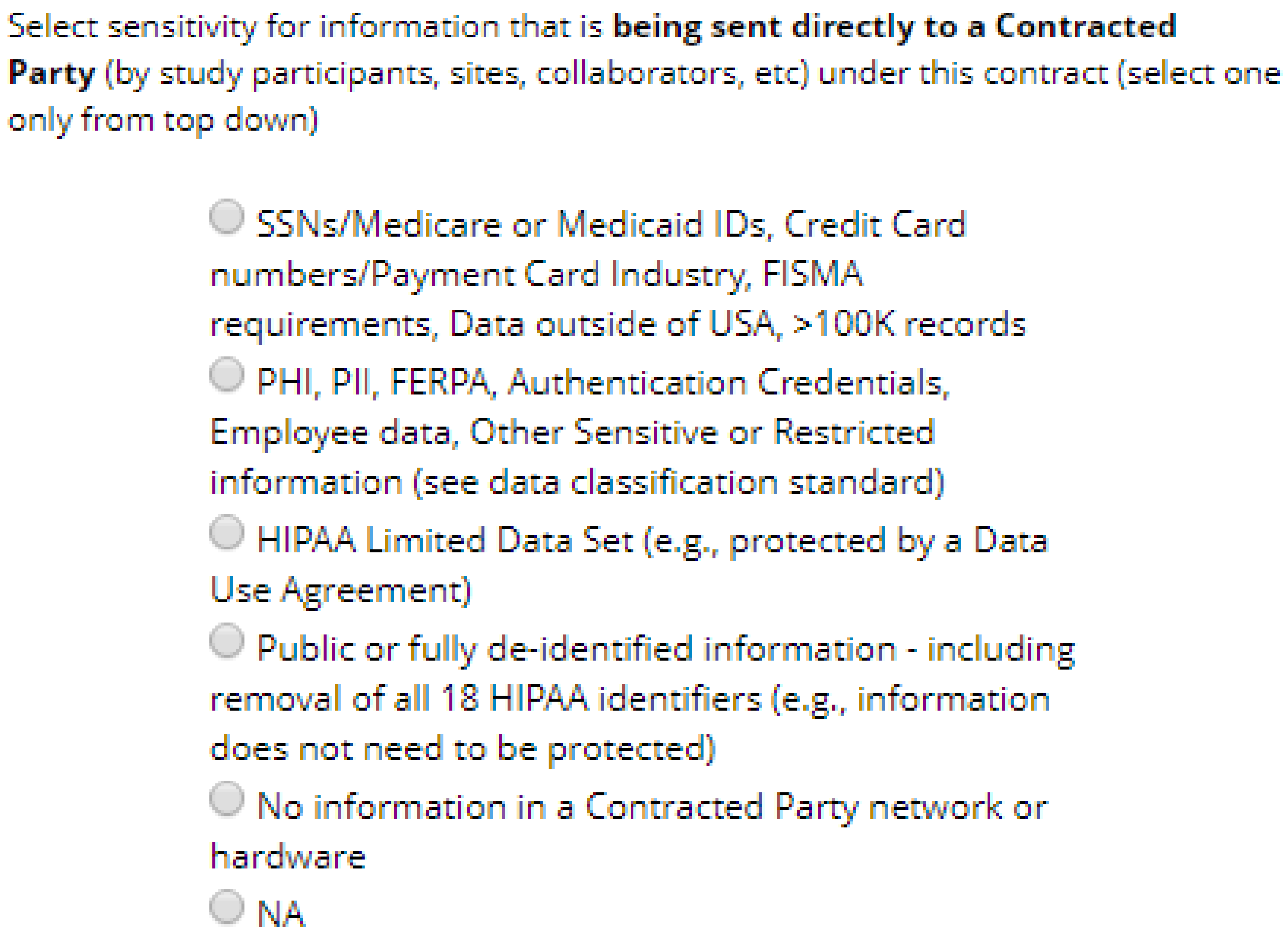
○ PHI, PII, FERPA, Authentication Credentials, Employee data, Other Sensitive or Restricted information (see data classification standard)

○ HIPAA Limited Data Set (e.g., protected by a Data Use Agreement)

○ Public or fully de-identified information - including removal of all 18 HIPAA identifiers (e.g., information does not need to be protected)

○ No information in a Contracted Party network or hardware

○ NA



Select sensitivity for information that is **being sent directly to a Contracted Party** (by study participants, sites, collaborators, etc) under this contract (select one only from top down)

○ SSNs/Medicare or Medicaid IDs, Credit Card numbers/Payment Card Industry, FISMA requirements, Data outside of USA, >100K records

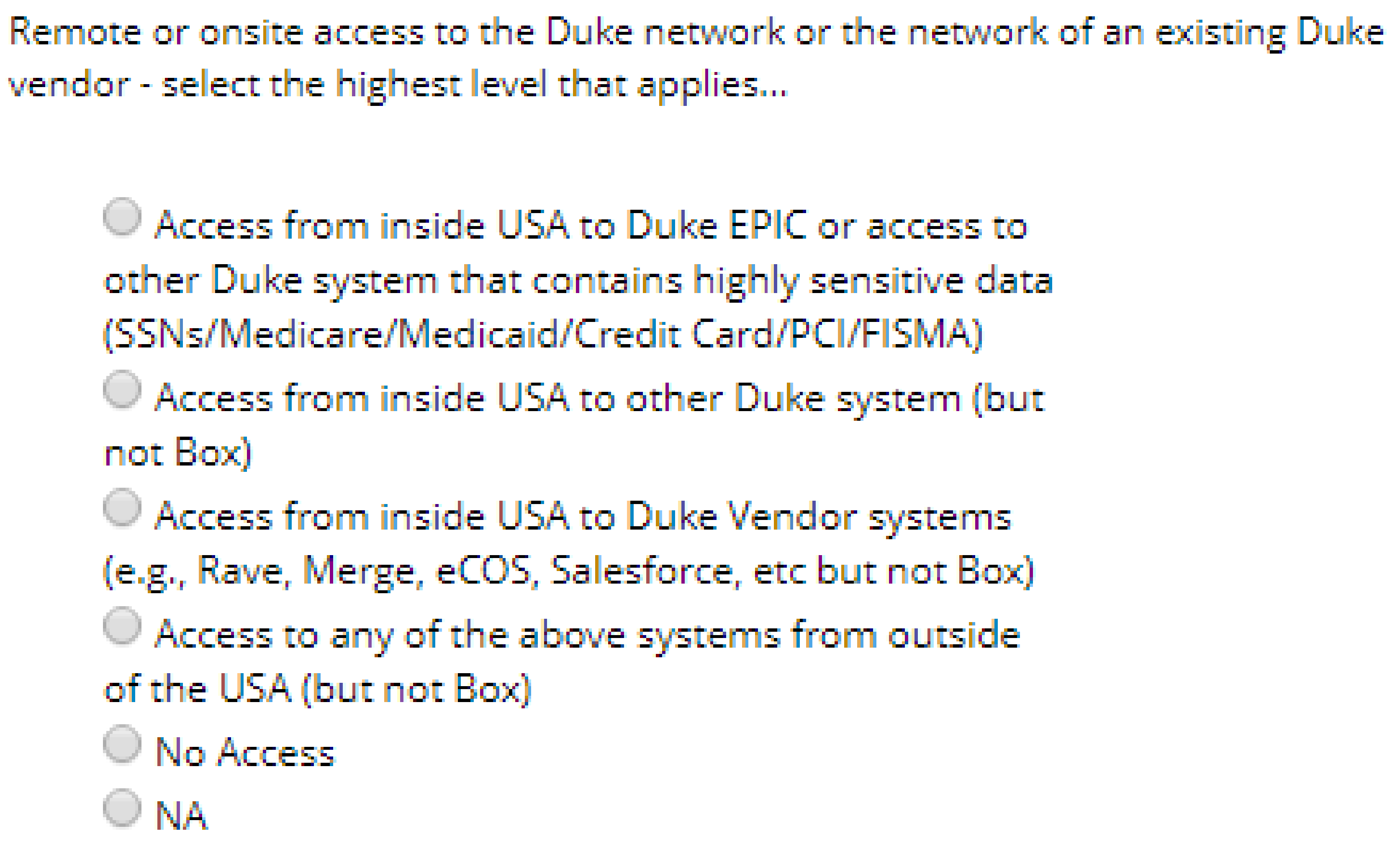
○ PHI, PII, FERPA, Authentication Credentials, Employee data, Other Sensitive or Restricted information (see data classification standard)

○ HIPAA Limited Data Set (e.g., protected by a Data Use Agreement)

○ Public or fully de-identified information - including removal of all 18 HIPAA identifiers (e.g., information does not need to be protected)

○ No information in a Contracted Party network or hardware

○ NA



Remote or onsite access to the Duke network or the network of an existing Duke vendor - select the highest level that applies...

○ Access from inside USA to Duke EPIC or access to other Duke system that contains highly sensitive data (SSNs/Medicare/Medicaid/Credit Card/PCI/FISMA)

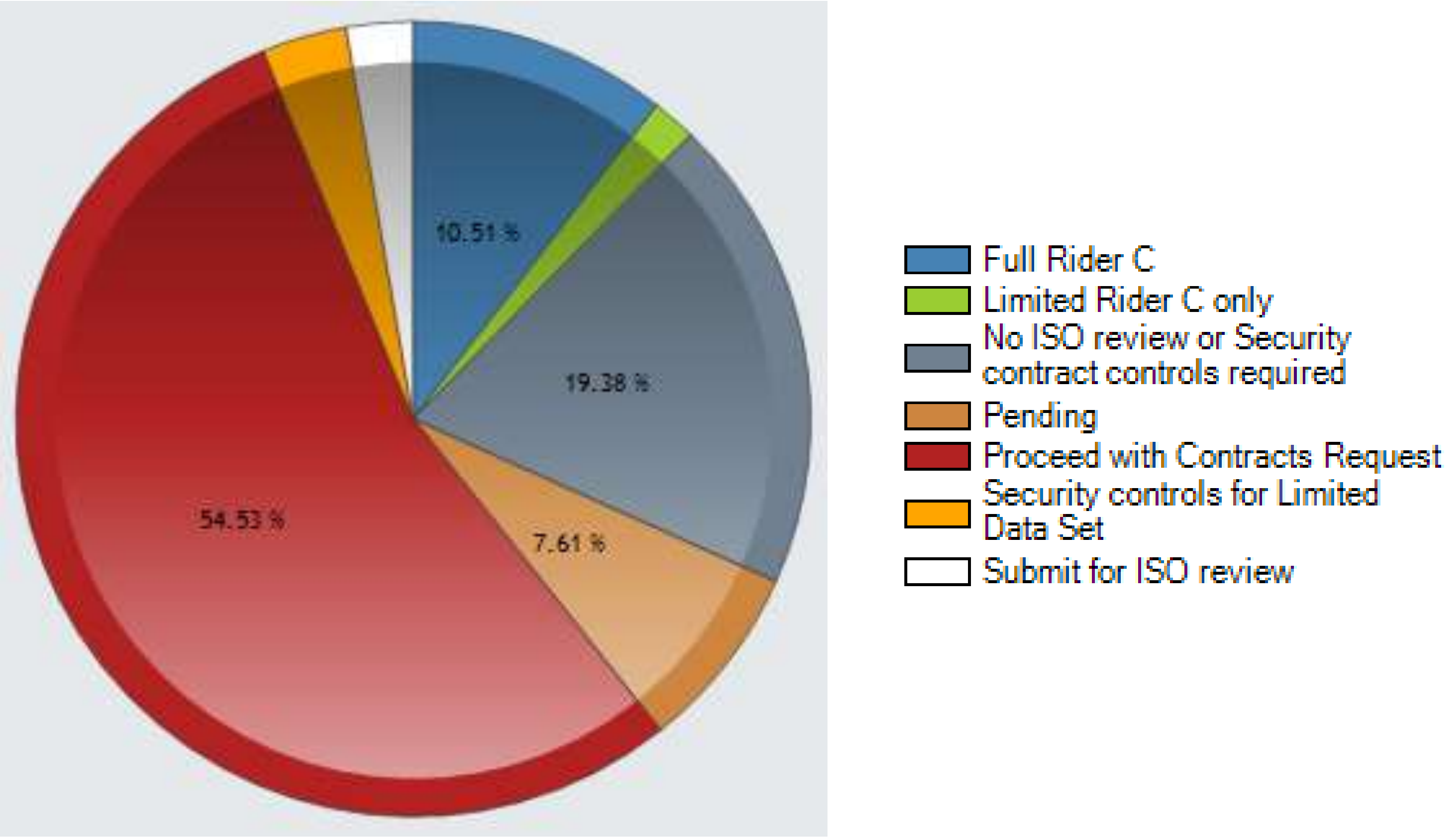
○ Access from inside USA to other Duke system (but not Box)

○ Access from inside USA to Duke Vendor systems (e.g., Rave, Merge, eCOS, Salesforce, etc but not Box)

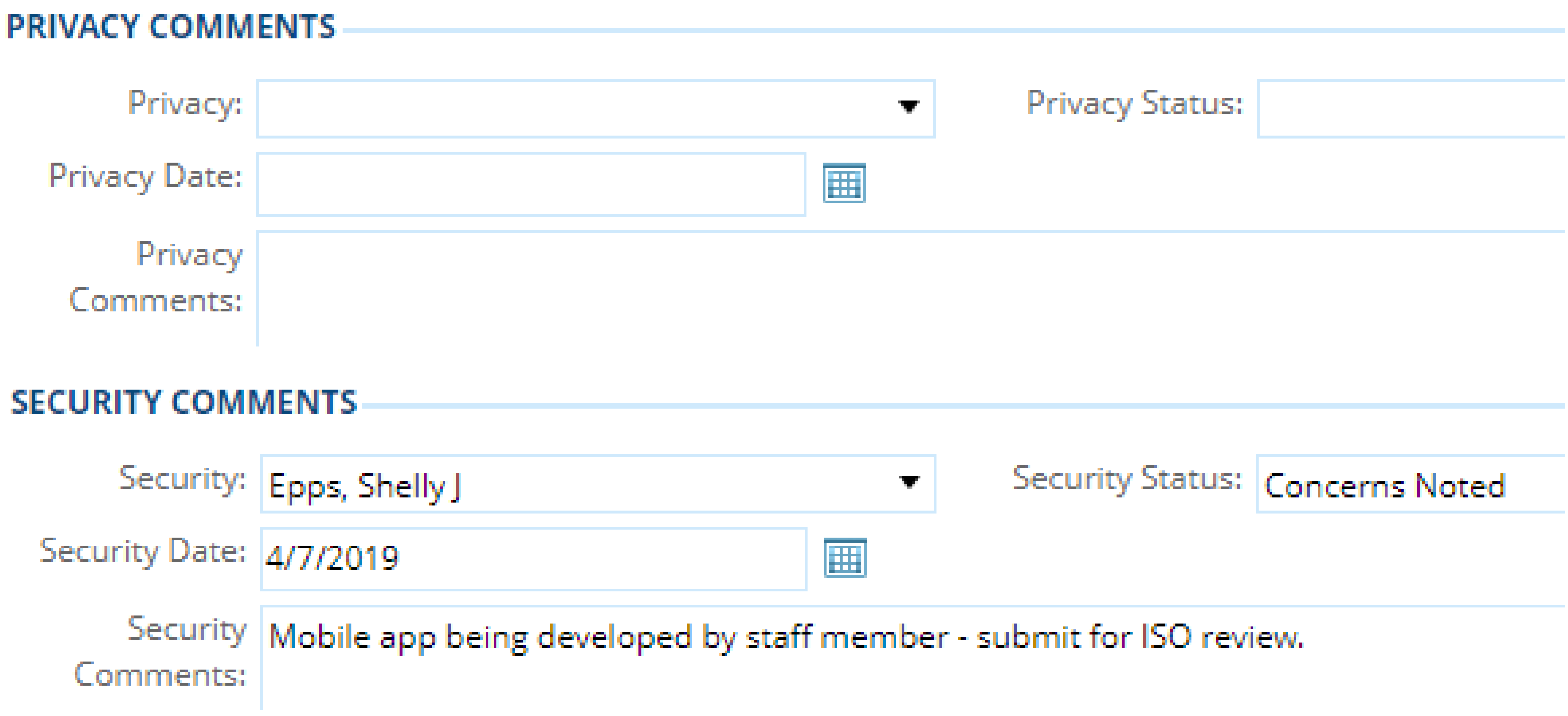
○ Access to any of the above systems from outside of the USA (but not Box)

○ No Access

○ NA



Increase Transparency to End-Users



PRIVACY COMMENTS

Privacy:

Privacy Status:

Privacy Date:

Privacy Comments:

SECURITY COMMENTS

Security: Epps, Shelly J

Security Status: Concerns Noted

Security Date: 4/7/2019

Security Comments: Mobile app being developed by staff member - submit for ISO review.

- Train your end users and reviewers to use the system and document it with easy to understand instructions.
- Use a platform with a well supported, simple to use UI. Limit changes to 2X yearly (at most!).
- Have a responsive/ engaged/ trustworthy person(s) involved with the knowledge and willingness to assess and override for outlier use cases.

Duke UNIVERSITY

DukeHealth Information Security

NIST
National Institute of Standards and Technology
U.S. Department of Commerce
NIST
FISMA
FEDERAL INFORMATION SECURITY MANAGEMENT ACT
Are you sure you don't have CUI?
CONFIDENTIAL
TOP SECRET
SECRET
CUI
Controlled Unclassified Information
COMPLYUP.COM

Assessing Risk for Research Grants

- NIST Framework
  - Now required by most State and Federal sponsored research projects
  - NIST 800-171
    - CUI – Controlled Unclassified Information
    - 109 Security controls
    - Normally for non-fed entities doing work for feds
  - NIST 800-53
    - FISMA
    - 303 Security controls
    - Normally required for federal entities
  - Most North Carolina agencies require NIST 800-53

- NIST Assessments
  - Time intensive
  - Labor intensive
  - Complicated
  - Don’t scale with Security Office resources
  - CSET tool is helpful but not fantastic!

How do we share the wealth?

- Who can be trained on CSET?
- Departmental IT? – Yes
- PI? – Probably not
- PI staff? - Maybe

What are the risks if assessments done incorrectly?

- Incomplete/inaccurate assessments
- Trigger an in-depth audit
- Fines or loss of funding
- Loss of reputation

Assessing Vendor Risk

- Things we look for:
  - SOC 2/Type II or answer 31 questions based on HECVAT
  - Breach History
  - Manual review of company and product
- Other resources:
  - HECVAT
  - Vendor assessment firms (BitSight, Security Scorecard)
  - Terms and Conditions
- Other questions:
  - What if vendor doesn’t respond?
  - Do their responses look “canned” or “borrowed”?
  - What if the security isn’t comfortable with the results of the assessment?
  - Who assesses the assessor?

Discovering Buried Risk

- Recent Discoveries
  - Contracts have been signed attesting that we were in compliance with certain regulations, when we were not.
  - Software or hardware was purchased years ago and is housing sensitive information with no risk analysis performed.
- Caught during the procurement process (renewals, etc.)
- Triggers requirement for risk assessment
- Delays cause confusion and angst (What’s the problem?? We are already using it!)

Can we really offload risk?

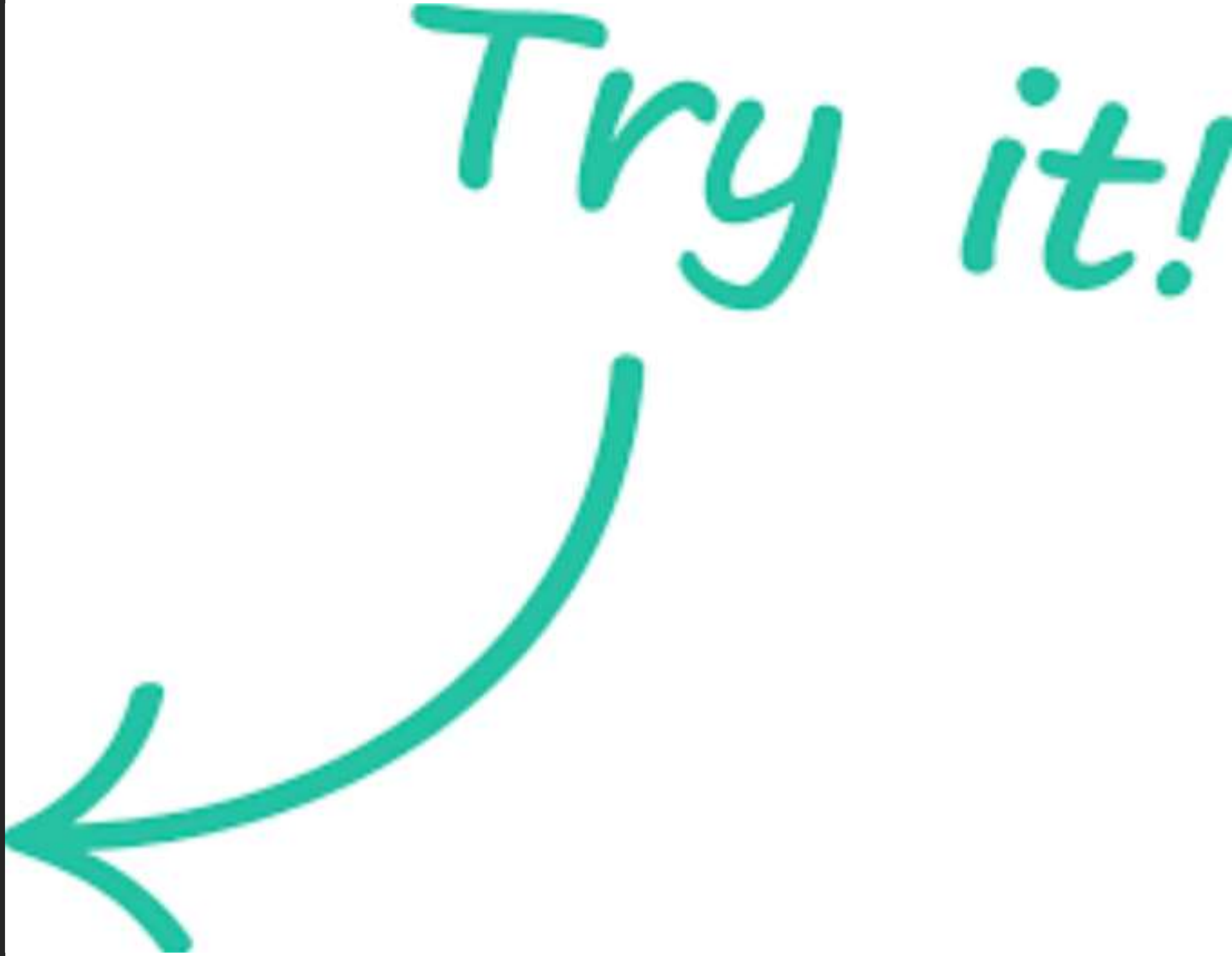
- We can offload risk assessment work, but the institution ultimately assumes the risk.
- Example:
  - School wants to buy an application to handle patient information.
  - Risk team performs assessment and finds the application to be high risk.
  - CISO does not approve. CIO agrees.
  - Dean of school insists and agrees to sign document stating that he will take responsibility for the risk.
- If there is a breach, the University’s reputation will suffer as well as the School.

Discussion Case 1:

Researcher indicates that their sponsor is requesting that they use a sponsor owned tablet that is HIPAA compliant to collect data using a pre-installed mobile app that will automatically send the data to their designated EDC provider.

What additional questions would you ask?

How would you scope and/or mitigate risk?

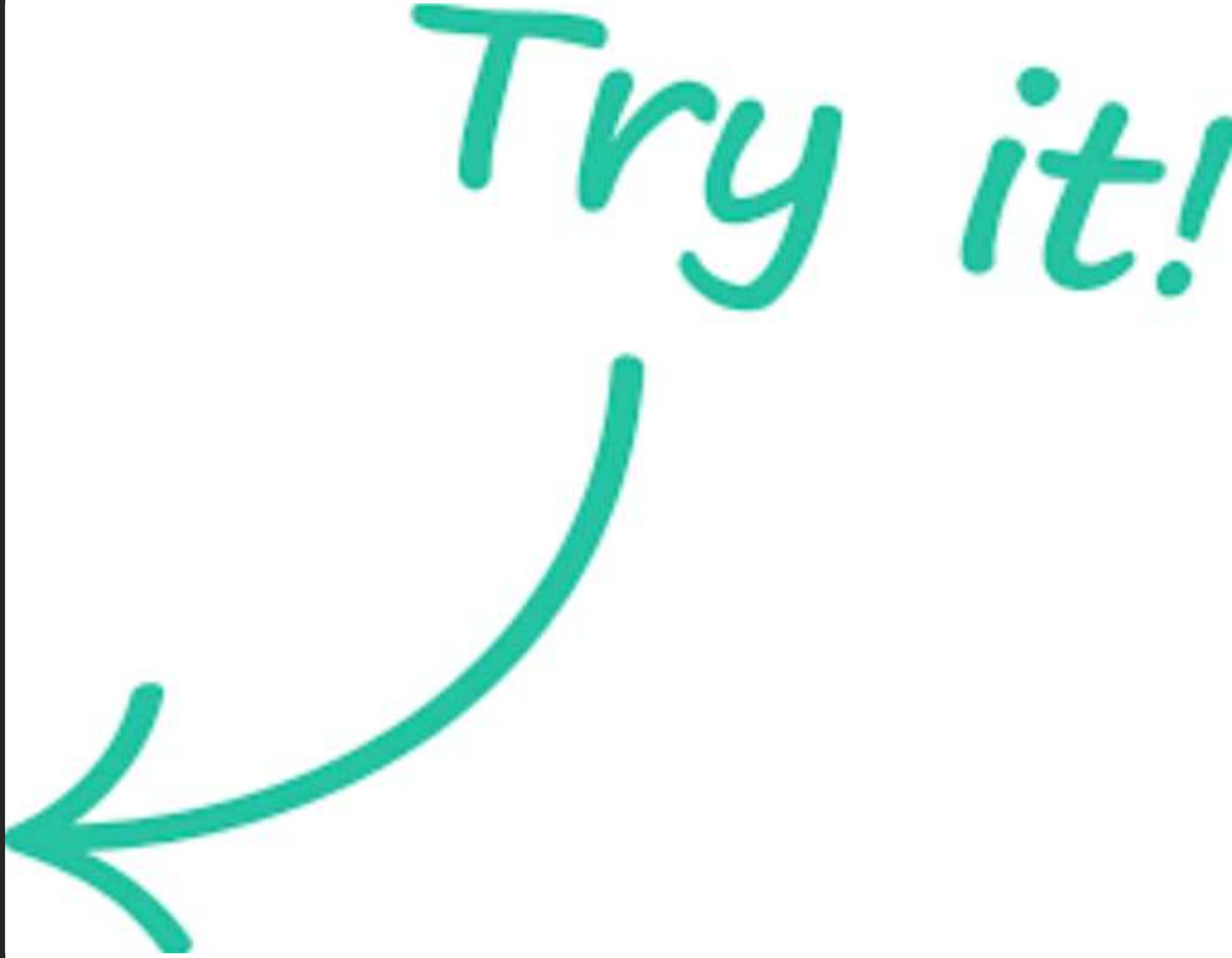


Discussion Case 2:

Neurology resident employed by your company has developed a mobile app decision support tool. She wants to do a research pilot with the intent, if successful, to eventually integrate with your institution’s instance of MyChart.   Data (including diagnoses and MRN) will flow in one direction (inwards).   Decision tool will be installed on company owned devices.

How would you scope and/or mitigate risk?

Would your assessment change if the resident indicated that she had received commercial seed money to fund a start-up to commercialize the tool?



Discussion Case 3:

Investigator initiated research proposal suggests studying the impact of using user-generated data and tailored messaging on weight loss.   The study will allow users to send data from wearables and popular diet and fitness apps that they are already using to a centralized, internally hosted dashboard and will tailor SMS messages to user provided phone number based on input.

What additional questions would you ask?

How would you scope and/or mitigate risk?