UNC
INFORMATION
TECHNOLOGY SERVICES

THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

ITS MANNING
CAMPUS BOX 3420
CHAPEL HILL, NC 27599-3420

T 919.445.9400
F 919.445.4545
its.unc.edu

Minutes
Enterprise Data Coordinating Committee
Regulatory Subcommittee
7/18/2017

Attending: Nicholas Graham, Kevin Lanning, Micki Jernigan, Lee Bollinger, Phyllis Petree, Allison Legge

Minutes:

- Welcome, announcements

- Discussion of initial topics and committee planning

Discussed list of likely committee topics:

- Creating a standard form for data requests
- Managing the lifecycle of MOUs
- Audit of data sharing agreements
- Data preservation guidelines (or requirements) For situations when vendors are keeping data on our behalf, how do we limit re-sharing, and require preservation?
- Providing guidance, perhaps in matrix form for our users about what is and is not acceptable for regulated data. This would match things like IRB levels, Risk classifications, Data Classification, NIST 171, GDPR, into context.
- Tool CSET by CERT and Homeland Security: to allow people to select data types and reviews and frameworks and regulatory schemes to deal with. Right now for us, this is a labor-intensive process in both Privacy and Security (and elsewhere) for humans trying to understand their data environment. Examine this tool for potential application or replication here.
- Discussion of what goes into risk rating.
- DAQ process updates.
- Distinguishing Data Steward responsibilities: “yes/no” for regulatory determination versus evaluating risk and determining “risk tolerance.” Is risk tolerance appropriately in the hands of data stewards or should that be abstracted to an institutional tolerance or a large data category (Trustee?)
- How we come to a risk scale, developing a grid: “Compelling need or benefit” Creating thresholds/hurdles/gates to evaluate “yes.” Evaluating sensitive information by classification, “how sensitive.”
- Collaborating with the IRB to build a framework for evaluation.
- Can we re-use some evaluation framework existing in another section (IRB, Student, other).

- What are peers doing?
- Company “Prevalent” working with EDUCAUSE. On-demand Risk Assessment/rating. Looking for a system-wide purchase effort. For the UNC system, getting NDA covering all schools to allow sharing of completed risk assessments between UNC schools. EDUCAUSE sponsoring a questionnaire that can become an industry standard for us.
- Evaluating use of SSN. Noting that “sensitivity” to SSN use is much lower for most people when an individual’s own SSN is not involved.
- Examine NC ID and Red Flag rules. PHI has tended to subsume people’s attention to SI.
- Addressing the need to continually assess risk, not just one time.

Preferred topics:

- How would we go about setting up to audit existing data use agreements? The Committee agrees that this is a good foundation, a big-picture item and an opportunity to capture low-hanging fruit. Identifying large data categories to audit. The committee discussed ensuring that the activity is not punitive. Identifying needs rather than finger-pointing.

- Look at what peers are doing. Ways we might gain efficiencies of scale. Improve our situation/minimize risk with better processes.

- Improve DAQ process.