District of Columbia Interagency Data Team

September 12, 2018

2:00 PM – 3:30 PM

Office of Chief Technology Officer

200 i Street SE

Washington DC, 20003

Conference Rooms 1001A & 1001B

Agenda

- ***Welcome, News & Updates***
  Michael Bentivegna, Data Visualization and Analysis PM, Office of the Chief Technology Officer

- ***Privacy Advisory Working Group***
  Turna Lewis, Privacy Counsel, Office of the Chief Technology Officer

- ***Health Insurance Portability and Accountability Act of 1996 (HIPAA)***
  Phillip Husband, General Counsel and FOIA Officer, DC Health (formerly DOH)

- ***Family Educational Rights and Privacy Act of 1974 (FERPA)***
  Darrell Ashton, Assistant Superintendent of Data, Assessment, and Research (DAR),
  Office of the State Superintendent of Education

Meeting Notes

Best attempt to capture notable comments and questions from attendees (paraphrased).

Presenter: Michael Bentivenga (OCTO) – Welcome and News

- Round of introduction
- Interesting question for the group, what is the most recent software you used today.
    - Majority of team answered Microsoft Excel followed by Tableau. And of course, Microsoft Outlook.
- Tableau Production version 2018.1.1
    - Major upgrade to move to 2018.2
    - Hold off on Desktop upgrades
    - Tableau Public (DC) w/automated ETL updates
    - Hyper not currently supported by Informatica Tableau extension at this time
    - Met with Tableau President and CEO Adam Selipsky (spelling?)
- MicroStrategy Production Version 10.11
    - MicroStrategy Dataset connector - connecting existing enterprise dataset (PeopleSoft, Procurement, QuickBase, etc.) to any other dashboard in the agency's own MicroStrategy projects based on the user's security definition.

Presenters: Turna Lewis (OCTO) – Privacy Advisory Working Group

- Office of Auditor – recently issued an audit report stating "DC government must improve" implementation of privacy compliance
    - DC lags behind private sector because we lack technology infrastructure
    - Auditor found that compliance and policies varied across DC agencies. Only federal oversighted agencies have these in place
- I was hired to and asked to look and identify policies needed
- Created this small working group containing only six members of privacy officers. Each with different areas of the expertise to get a good cross section
- First meeting was held in July 2018
- We are working to create a *Privacy Awareness 101* training
    - how to work with privacy and data
    - how it's disposed
    - It will be mandatory for all DC employees to attend this in future
- First, we will handle Personally Identifiable Information (PII)
- Then, we will do policies on data dreach
- *Question*: have you thought much about biometric data? For example, OCTO and MPD have cameras.
    - Yes, it is something that needs to be included in this assessment and working group. Example, facial recognition. Programs like Smart Cities are ahead of the privacy policy

- *Question*: you mentioned data breach. MPD is particular interest to this. Have you considered two factor authentications?
    - That it is an issue we have done research on. It is difficult to implement city-wide but yes OCTO is very interested in that as generally related to cyber security.
- The group is also looking at either cities. Seattle is a gold standard model right now. Any time there is a technology that touches PII then there is a public hearing.
- *Question*: do you have recommendations on training?
    - We are going to look at what is the baseline training for PII. Then look at specialized training.
- *Comment*: the Office of the State Superintendent of Education (OSSE) does have training and data breach policies in place.
    - That is true, agencies that must follow federal laws already have these in place

Presenter: Phillip Husband (DC Health, formerly DOH)– HIPAA

Note: Phillip Husband lead a conversation on this top and presentation slides are not available.

- Before HIPPA – hospitals were discarding records in trash and private companies were mining data without regulation
- Once HIPPA wasa enacted, DC government implemented coverage for only agencies that were required by law. It was too expensive to implement in all of DC.
- Federal penalties are substantial, starting at 250k
- *Question*: what does it cover and who can get it?
    - Think of it like a colander. Solid structures and holes where some covered and some not
    - Covers something that is identifiable to you, the individual: name, home address…
    - Covers insurance plans
    - Includes groups that are clearing houses
    - Electronic billing
- HIPPA is actually a minimum requirement. There are examples of states with higher policies. For example, DC government holds HIV data is very strictly held
- Everyone thinks DC Health is heavily regulated (?)
- PHI – public health information could be different
    - Some data can be shared without your consent. An example, immunization records (this should be confirmed)
    - If you want PHI, depends on what you ask. Usually you'll get redacted. But even redaction is not always enough. It is based on what you're looking for, who are you, and what are you going to do with it.
- *Question*: can we talk about the aggregation? It looks like the denominator has to be 20K people… can you talk about what's allowed for aggregation? But example, many census tracts do not meet this.
    - Sometimes you can go down to a population of 10k. some of our DC health internal aggregation is done at 10k.
- HIPPA is a law supplemented by state law

Presenter: Darrell Ashton (OSSE) – FERPA

Note: the FERPA presentation slides are very detailed. Visit https://octo.dc.gov/node/1368191.

- FERPA spells out the rights of parents and guardians with regard to their children, students. It is data collected within and education environment or setting. Maintained by an educational agency or institution. There are two definitions/types
    - *Education record* could be in any formation – pictures for yearbooks, someone's handwriting, video… (see more in slides)
    - *Personally Identifiable Information* is data that is directly linked to ONE student – SSN, date of birth, address, parent's name… (see more in slides)
- Penalties are high,
    - Could withhold federal funding
    - Terminate eligibility for any funding of any program
    - Issuing cease and desist orders
    - OSSE could be liable for breaches of other institutions it shared data with
- OSSE does have hard data sharing agreements with some entities like other DC agencies
- OSSE is the custodian and steward. If parents ask for their child's student data then they must go to their school as official source.
- Bus routes of students are private, it could tell you where their address is or information of that neighborhood
- Student scores on any assessment, disciplinary actions
- How can OSSE shares data
    - Yes, sharing is permitted under some circumstances – (check slides)
    - Lawyer or court order
    - Written sharing agreements under legal exception…
- *Question*: what are the legal exceptions?
    - This is where there is a gray area. There are two main ones: authorized representative with for example parental consent. Also, research studies on behalf of schools.
- I (Darrell Ashton) personally review all agreements down to the details of all data elements that can be shared. Once data is shared then I also look at all data elements that should match documented agreement.
- OSSE no longer has unending data sharing agreements. All have an expiration. Usually a year max. We have the right to go into your work and monitor and make sure you are compliant.
- OSSE has templates you can use if you request data.
- If you intend any public disclosure of the data then you first have to show OSSE what you'll be sharing publicly… OSSE must agree it is compliant.
- *Question*: do you have specific requirements for data destruction?
    - We do not have those, and we just go on case by case. We work with the agency or institution to ask what is it that they intend to do.

- *Question*: regarding student travel time to school. What level of aggregation would we need to do in order to publicly share? Is there a magic number? It would be a wonderful thing to work towards standardizing suppression levels.
    - It depends. And I know that is not a good answer. Many things we suppress to 20 students groupings (this should be confirmed). Department of Education provides some wide latitude to decide what is appropriate. OSSE decides in order to protect but also to bring value to data research and studies.
- *Question*: OCTO is working to provide kids-ride-free cards. Is this considered FERPA data?
    - Maybe and maybe not. But you could argue that this program is used to address school attendance. That might be an exception.
- *Question*: would you share your templates?
    - Yes, we can share OSSE's templates
- *Question*: what kind of practices do you have in-house?
    - Every single employee is required to sign a Non-Disclosure Agreement (NDA)
    - All employees required to go to an in-person Personally Identifiable Information (PII) training
    - All employees required to go to regular re-training and certification
    - By default, no one except people on my team and OSSE IT shop have access to the data. Even as internal employees at OSSE
- *Question*: suppression topic… there is no standard suppression number, process and it is case by case?
    - Yes, we would tell you off the bat what rules would be but yes we review case by case as well
- *Question*: are some data attributes more sensitive than others? Location data versus OSSE student identifier numbers?
    - We view these as the same sensitivity. The only exception would be SSN – absolutely not shared
- Additional resources: (look at slides)

Note: the FERPA presentation slides are very detailed. Visit https://octo.dc.gov/node/1368191.

Meeting adjourned

Next meeting tentatively scheduled for November 2018