I am Lisa Neidert, Director of Data Services at the Population Studies Center, University of Michigan

We run a full service restricted data shop – providing lots of concierge services that are really only practical for a research unit, not a campus-wide enterprise at least at our staffing.

I am not going to emphasize all of our tools we have because they are probably overkill if you are just setting up or beefing up restricted data services.
Our tools evolved into a database once the number of data providers and contracts got too much for my memory and filing system.

We currently have 49 active contracts with 74 unique users. Over time we have had almost 40 different data providers and it was this number that drove us to develop a contracts database.

Data providers can & do have their own conditions – both legal and security and you need to be able to keep track of that as well as all of the administrative details – dates, users, media.
But, no matter how small your shop is, including a researcher who is keeping track of his/her 2 or 3 contracts, you need to:

Set up the secure data environment that you described in your data protection plan

Keep track of the expiration date of the contract & reporting dates, if applicable

Keep track of collaborators or students who may be added/removed from the contract

Keep track of the media

And follow the contract conditions. Do you know where your contract is? Did you read it? What does it say about disclosure conditions? Maybe nothing or maybe that paper that was presented last week at PAA needed a disclosure review first.
Most of the audience, including me, need help with setting up a secure environment.

Almost all universities had a central IT operation that has a website that describes different kinds of data and related security problems and solutions.

However, IMO these have all been developed without any reference to restricted data contracts.

In fact they are authoritative enough that a user/librarian could be suckered into just handing off the secure environment to IT folks.

You cannot do that. You need to let them know what you said would in your data protection plan and what the contract allows.

And, going back to contract conditions some data providers have limits on the number of signatures on a contracts.

**TO DO LIST**

- What you can/must do – without bells & whistles
  - Set up computing environment
  - Monitor Expiration/Renewal dates
  - Track user(s)
    - Adds/Deletes from contract
    - Affidavits
  - Track Media (type; receipt date/return date)
  - AND FOLLOW THE CONTRACT
The UM data security website lets you choose what kind data you need to protect and get a report back with the allowed (green light) and disallowed (red light) services.

So if I put in sensitive human subjects data here’s what I get as my report
Go to next slide to show pitfalls
Now many of these services are not allowed by data protection plans. Specifically, most do not allow back-ups; cloud storage; or sharing the data.

It is up to you to communicate your needs to the IT experts.

You are responsible for following the contract.

On the other hand, many data providers need to be more flexible. Frankly, I would prefer a secure LAN rather than a multitude of stand-alone computers, each of which are vulnerable to disk failure and are an inefficient use of CPUs.
Some of our contracts have been active for over 10 years and we have 15 to 25 CDs for these contracts.

I track the media by its label, which is not always provided; date we got it; date we returned it; and if applicable a password.

And I have a notes field to remind me of other events related to the media.

This started out as an Excel file for each contract. It doesn’t have to be fancy. But, you have to track your media.

And, if data come via a secure download, note that so you won’t panic when you can’t find media to return/destroy.

We have a field that says where the media are stored (under my control, the researcher’s control or secure download).
We have some automatic functions in our database, which allow us to run reports so we know which contracts are expiring. We clarify with the PI on whether they want to extend it or close it about 2 months before the expiration date.

And be careful with BLS. For those contracts, the PI is a “temporary agent” of BLS. BLS takes this quite seriously and won’t extend these contracts for 10+ years. The PI has to start with a new project, perhaps building on his/her previous work.
We also emphasize contract conditions to our users. In fact, education and communication with our users is my most important function.

Contracts vary in the conditions they impose.

The contracts are not user friendly. The conditions are not in the same order across contracts so it is hard for a researcher to even find the disclosure clauses, if they even exist.

So we have parsed all of our contracts and put this detail in our database. We then create a structured contract so that the conditions are presented in the same order across contracts – assuming the condition exists.
Here is an example of a contract condition email. We send this out before the user gets access to the data and then once a year as a reminder.

We also send out a security conditions email to keep it short.
It is important to make sure researchers know what the contract conditions are because many of these conditions are not aligned with how researchers do their jobs. These are highlighted in pink.

There is a tension between a researcher’s mind set/independence and many contract conditions.

Our researchers are very good about following contract conditions because they know they have to. But, that’s why it is important to make sure they know what the conditions are.
And to make things more complicated, sometimes conditions of use are not in the contract.

Here are examples of clauses that are in the “application process” or in the data protection plan application instructions.
Here is our restricted contracts portal. We have 4 links that might be useful as a resource. [URL embedded in the slide]

The first is a grid that compares all contract conditions by data provider.

The second is links to the application process and to the contracts for our data providers  
The third link allows you to produce a comparison report for contracts such as “disclaimer language.” “Build your own”

The fourth link shows inspection reports for two data providers. These are good practice documents to use in-house.
Here’s an example of the contract conditions across all of our data providers.

It is a bit overwhelming and too small to see, but the rows are the conditions and the conditions researchers ought to care about are at the top.

The data providers are the columns and they are sorted by type of providers: academic, bio-medical, federal, non-profit, state/local and even a few public data agreements.

The x indicates that this condition exists for that contract and if you click on the x you see the contract language.

If you click on the data provider name at the top, you get the structured contract.