Responsible Conduct of Research Workshop Series, 2015-2016

Record Keeping, Data Management, and Sharing of Information

-- November 11, 2015--
Expectations

- **Read the Syllabus for each Workshop**
  - Pre-Workshop Readings and completing the Pre-Workshop Tasks are important for identifying the issues and questions that are most important to your interests.

- Because these sessions are designed to promote discussions, **no cell phones or laptops will be allowed on desks or be used during the workshops.**

Adapted from: Ebert-May and Hodder (2008) Pathways to Scientific Teaching (Chapter 1)
Last Time

- "Discuss with your research integrity consultant the meaning of plagiarism, self-plagiarism and his/her recommendation(s) for how to avoid unintentional plagiarism."

- "Consider for yourself when and how you should properly credit others for their ideas and research/scholarly work AND when and how YOU wish to be credited for your work."
Please indicate your current status at MSU

1. Early (first years)
2. Mid (middle years)
3. Late
4. Postdoctorate
5. Faculty
6. Other
Were you able to discuss plagiarism with your research integrity consultant as requested?

1. Yes
2. No
For only those who answered “Yes”. Were “recommendation(s) for how to avoid unintentional plagiarism” helpful?

1. Yes
2. No
Plagiarism is always intentional

1. Agree
2. Disagree
In 2011 Tilburg University suspended Stapel, pending further investigation, for fabricating and manipulating data for his research publications. This scientific misconduct took place over a number of years and affected at least 55 publications.


June 1, 2013
“The committee, which interviewed dozens of Stapel's former students and colleagues, concluded that Stapel acted alone. The report says he would discuss experimental designs in detail with collaborators and would claim to conduct the surveys at high schools and universities with which he had special arrangements. The experiments, however, never took place, and Stapel gave collaborators made-up data sets, investigators allege. In other instances, the report says, he told colleagues that he had an old data set lying around that he hadn't had a chance to analyze. When Stapel did conduct actual experiments, the committee found evidence that he manipulated results.”

“Many of Stapel's students were simply given data to analyze and graduated without having ever run an experiment, the report says. The commission writes that Stapel was “absolute lord of the data” in his collaborations. Colleagues or students who asked to see raw data told the commission they were given excuses or even threatened and insulted.”

November 13, 2011

Fraud Scandal Fuels Debate Over Practices of Social Psychology
Even legitimate researchers cut corners, some admit

By Christopher Shea

The discovery that the Dutch researcher Diederik A. Stapel made up the data for dozens of research papers has shaken up the field of social psychology, fueling a discussion not just about outright fraud, but also about subtler ways of misusing research data. Such misuse can happen even unintentionally, as researchers try to make a splash with their peers—and a splash, maybe, with the news media, too.
Even before the Stapel case broke, a flurry of articles had begun appearing this fall that pointed to supposed **systemic flaws in the way psychologists handle data.**

"If high-impact journals want this kind of surprising finding, then there is pressure on researchers to come up with this stuff," says Mr. Wagenmakers, an associate professor in the psychology department's methodology unit [Eric-Jan Wagenmakers, of the University of Amsterdam].

Bad things happen when researchers feel under pressure, he adds—and it doesn't have to be Stapel-bad: "There's a slippery slope between making up your data and torturing your data."

In September, in comments quoted by the statistician Andrew Gelman on his blog, Mr. Wagenmakers wrote: "The field of social psychology has become very competitive, and high-impact publications are only possible for results that are really surprising. **Unfortunately, most surprising hypotheses are wrong. That is, unless you test them against data you've created yourself.**"
Diederik Stapel loses teaching post, admits he was sockpuppeting on Retraction Watch

Diederik Stapel’s reinvention as a teacher at a college in the Netherlands has proven to be short-lived.

“Stapel also admitted today that he had been leaving comments on Retraction Watch using a fake name, “Paul,” and referring to himself in the third person, which we consider sock puppetry. While we welcome anonymous and pseudonymous comments, when we have reasons to believe that a commenter is to be violating our comments policy against unverified claims — as pretending not to be Stapel when you are actually Stapel would be doing — we will try to determine whether the comment is accurate as submitted”
DEFINITIONS

- Data OWNERSHIP: who has LEGAL rights to the data and holds onto data once project is complete.
- Data COLLECTION: the process of obtaining recordable, measurable endpoints
- Data STORAGE & PROTECTION: how and where data are physically or virtually stored and protected from theft or tampering.
- Data RETENTION: how long the data need to be stored according to regulations
- Data ANALYSIS: how raw data are modified for others to use and relate to
- Data SHARING: communicating data — at any level — to others privately or publicly
  - Guidelines for Responsible Data Management in Scientific Research, Clin Tools, ORI FUNDED
MSU Institutional Data

Institutional Data are all of the data and records held by the University, *in any form or medium*, for the administration, operation, or governance of the University or any unit of the University

- Confidential
- Public

[https://tech.msu.edu/about/guidelines-policies/msu-institutional-data-policy/](https://tech.msu.edu/about/guidelines-policies/msu-institutional-data-policy/)
MSU Confidential Data

(i) Institutional Data that could, by itself or in combination with other such Data, be used for identity theft or related crimes

(ii) Institutional Data whose public disclosure is restricted by law, contract, University policy, professional code, or practice within the applicable unit, discipline, or profession

(iii) Records of the University’s security measures

(iv) Institutional Data whose value would be lost or reduced by unauthorized disclosure or by disclosure in advance of the time prescribed for its authorized public release, or whose unauthorized disclosure would otherwise adversely affect the University financially.
Confidential Data Examples

- Individually identifiable medical data
- **Human subjects research data**, if the subjects have been promised confidentiality
- Proprietary business data owned by a third party and provided upon a promise of confidentiality in a NDA
- Proprietary computer applications/code to which the University holds a license that restricts distribution
- **Exam questions and answers/scoring keys** which the professor has not released as Public Data
- Research data or results prior to publication or the filing of a patent application
- Non-patentable technical information/know-how that enhances the value of a patented item or has independent commercial value
MSU Public Data

Institutional Data that have become generally available to members of the public because a person with authority to do so has intentionally released or distributed them without restriction or limitation.
Members of the University community are individually responsible for the security and integrity of Institutional Data in their possession or control, including their proper storage and disposal.
Best Practices for Record Disposal

Remove (sanitize) confidential data from hard drives/disks before transferring/discarding using a utility like killdisk (Windows/Linux) or MAC OS utility

- Reformatting & reinstalling the OS is not sufficient
- Some media (e.g., paper, CDs) must be shredded

MAKE SURE YOU HAVE RETAINED COPIES OF DATA AS REQUIRED BY MSU, NIH, contract, etc.!!
Michigan Identity Theft Protection Act

- Requires that any records that contain any of the following types of Confidential Data in an unencrypted form be destroyed (shredded or erased) when such Confidential Data is removed from a University data system (and not otherwise needed):
  - Person's first name (or first initial) and last name in combination with that person's (a) social security number, (b) driver's license or state personal identification number, or (c) credit or debit card or other financial account number, in combination with any security code, access code, or password that would permit access to that financial account.
Hippa Data Breaches

Figure 1: HIPAA Data Breaches and # of Individuals Affected HHS Office for Civil Rights
HIPPA Data Breaches

- Average health data breach cost $6.6M
  - Fines, remediation, litigation
- A single breached laptop can result in fines up to $1.7M from Department of HHS
- Total cost of breaches $5.6B

- Financial ID worth $5-$10, whereas a medical ID can be worth 5-10 times that amount
What Happened to Data After a Breach?

- Fake Excel spreadsheet with 1,568 names, SSNs, bank account info, etc. was created.
- Within 2 weeks:
  - Stolen data was in 5 continents
  - Was viewed in 22 countries
  - Was opened more than 1,000 times
  - Was downloaded 47 times
  - Was posted to cybercrime marketplaces on the “Dark Web”
Best Practices for Record Retention

Encrypt all confidential data, both at rest and in transit

- And especially on USB drives!

Encryption Utilities include:

- 7-Zip (Windows)
- Symantec Endpoint Encryption (Windows)
- WinZip (Windows, MacOS)
- MEO (Windows, MacOS)
- Keka (MacOS)

Consider LastPass for password management

- https://lastpass.com/
Sharing Data

Recommended --

- Use FileDepot Internal (900MB)
  - Addresses Institutional Data Requirements
- Otherwise FileDepot (900MB)
  - Do NOT Use without encrypting sensitive Institutional Data

- https://filedepot.msu.edu/
Cloud Computing

What Cloud Services Can I Use?
Cloud Computing – MSU Google Apps

- MSU Google Apps
  - Better Terms of Service (**CORE APPS ONLY**)
    - MSU has contract for the “Click Through” Agreement
    - ToS designed to protect intellectual property rights and privacy
  - Logon with MSU NetID
  - [http://googleapps.msu.edu/](http://googleapps.msu.edu/)
Cloud Computing – MSU Google Apps

- MSU Google Apps include
  - Calendar
  - Drive & Docs
  - Sites
  - Classroom
  - Hangouts
  - Contacts

- MSU Google Apps
  - OK from FERPA perspective
  - “Google will be considered a ‘School Official’ and will comply with FERPA”
  - But make sure you DON’T Share FERPA data with Students, etc.
  - Watch your Permission Settings!!
Data Ownership

MSU owns all intellectual property rights to MSU's data, consistent with MSU's intellectual property policies.

The Agreement does not contain any transfer of license to Google for any user content in the ways that the Google Consumer ToS have sometimes done.
Cloud Computing – MSU Google Apps

Data Location

Google facilities that store and transmit data may be located internationally. MSU's Agreement does not constrain Google from moving or storing MSU data abroad.

What does this mean for your research data?
The Google Agreement is silent regarding backing up user data.

**ASSUME YOUR DATA ARE NOT BACKED UP**

Google does NOT provide recovery services for lost end user data. *MSU IT Services does NOT back up MSU data on Google services.*

**USERS MUST ASSUME INDIVIDUAL RESPONSIBILITY FOR REGULARLY BACKING UP DATA THEY STORE WITH GOOGLE**
Google apps are OK

- for classes
- for non-confidential data types
- for personal data files
- Research collaboration (*unless involves high consequence IP*)

- Not OK for most other types of Confidential Data
Data Management – Provider ToS

- Non-negotiated changes to terms of use, service & business model
- Transfer of license
- Security & privacy
- Back-ups
- Assured purging
- Data formats
- Indemnity
- See MSU “Appropriate Use of Cloud Computing”
Google Individual Privacy ToS

- Google uses information you provide & what they collect (& can change whenever they want)
  - Google profile
  - Device identifiers
  - Server logs & IP addresses
  - Location information
  - Unique application numbers
  - Local storage (cookies, etc.)
  - Combine data across multiple accounts
  - Pixel tags
Google Individual ToS

When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content.

The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones. This license continues even if you stop using our Services (for example, for a business listing you have added to Google Maps). Some Services may offer you ways to access and remove content that has been provided to that Service. Also, in some of our Services, there are terms or settings that narrow the scope of our use of the content submitted in those Services. Make sure you have the necessary rights to grant us this license for any content that you submit to our Services.
Google Individual ToS

We may modify these terms or any additional terms that apply to a Service to, for example, reflect changes to the law or changes to our Services. You should look at the terms regularly.

All claims arising out of or relating to these terms or the Services will be litigated exclusively in the federal or state courts of Santa Clara County, California, USA, and you and Google consent to personal jurisdiction in those courts.
Definitions Review

- OWNERSHIP: Who has LEGAL rights to the data and holds onto data once project is complete

- STORAGE & PROTECTION: How and where data are physically or virtually stored and protected from theft or tampering
OWNERSHIP: Who Owns Data Placed in the Cloud?

- Need to look at ToS!
- MSU Google Apps Agreement

“Intellectual Property Rights: Except expressly set forth herein, this Agreement does not grant either party any rights, implied or otherwise, to the other's content or any of the other's intellectual property. As between the parties, Customer owns all Intellectual Property Rights in Customer Data, and Google owns all Intellectual Property Rights in the Services.” (MSU is the customer)
Definitions Expanded

- STORAGE & PROTECTION: If online, who really has access? How do they protect it?

- POSSESSION IS KING! IF YOU KEEP IT TO YOURSELF, IT’S YOURS
Other Data Management Issues

Transferring & Storing research data at an Internet based provider such as

- Box
- Prezi
Box ToS

- Except for material that we license to you, we don't claim ownership of any Content that is transmitted, stored, or processed in your account(s). We also don't control, verify, or endorse the Content that you and others make available on the Service.

- We provide functions that allow you to control who may access your Content. If you enable the features that allow you to share the Content with others, anyone you've shared Content with (including the general public, in certain circumstances) may have access to your Content.

- You will: (a) be solely responsible for the nature, quality and accuracy of the Content; (b) ensure that the Content (including the storage or transmission thereof) complies with these Terms and any and all applicable laws, and regulations; (c) promptly handle and resolve any notices and claims relating to the Content, including any notices sent to you by any person claiming that any Content violates any person's rights, such as take-down notices pursuant to the Digital Millennium Copyright Act and any other notices; and (d) maintain appropriate security, protection and backup copies of the Content, which may include, your use of additional encryption technology to protect the Content from unauthorized access. Box will have no liability of any kind as a result of the deletion of, correction of, destruction of, damage to, loss of or failure to store or encrypt any Content.
Prezi ToS

- **Prezi Public (free) Accounts.** If you have a Prezi Public (free) account, all of the content you create, including all of the information within your presentations, will be available to anyone who has access to the internet (“Public User Content”).

- Public presentations can be viewed by other Prezi users, will appear in the searchable Prezi database, and will be available for others to access and view online.

- Accordingly, **you hereby do and shall grant to each User and to the public a worldwide, non-exclusive, revocable license to access, view and publicly perform your Public User Content.**

- This license ends when you delete the presentation or your account is closed (either by you or by us), **except to the extent that the content has been shared with others and they have not deleted it.**
Other Ways to Share Research Data

- Keep it offline: Use removable storage like USB keys, portable disks (PROTECT & ENCRYPT THEM!)
- Use network service providers with an appropriately restrictive disclosure policy:
  - [https://afs.msu.edu/](https://afs.msu.edu/) and [https://netfiles.msu.edu/](https://netfiles.msu.edu/)
  - An Email system hosted at MSU such as [https://mail.msu.edu/](https://mail.msu.edu/) **IF you are sure all recipients are NOT forwarding mail off-campus**
  - MSU hosted services should be sufficiently restrictive
How to Know What is Safe

- Email is NOT always secure
  - Transport
  - Storage

- File Sharing: Do you trust the administrators? Why? What is their privacy policy? Reputation?

- Does the privacy policy sufficiently protect research data for your project guidelines?

- Question their motive: If the service is free, what does the provider gain from you? If the service is free, YOUR INFORMATION may be the product

- Think WikiLeaks
Miscellaneous Recommendations

☐ Keep at least two copies of worthwhile research data in two different places, or you really have none

☐ Don’t fall for phishing emails or popups
  - Verify or ignore
  - “Your mailbox size has reached quota limit, which is over 90% of your mail quota. Please click on the link below to verify your account to avoid exceeding your quota.”
Tips

- 5 Steps to Staying Secure
  - YOU (phishing, web sites)
  - Updating (stay current)
  - Passwords (strong, 2-step verification)
  - Encryption (data at rest and in motion)
  - Backups (data stored in multiple locations)

- From: http://www.sans.org/tip_of_the_day.php
Paranoia is GOOD!

- We know what you are doing.
- We know where you are going.
- We have your bank details.
- We are watching you.
Record Keeping - REPRODUCIBILITY

- Keep thorough notes (strain of animals, source; full name of drug, source and lot #)
- Note errors made!
- Keep track of dates and times: DISCOVERY!
- Keep track of people and their contributions
- Make original entry in pen or time stamp your original entry electronically

- Guidelines for Responsible Data Management in Scientific Research, Clin Tools, ORI FUNDED
There are two types of data – **Quantitative** and **Qualitative**. The primary types of data supporting my research are:

1. Qualitative
2. Quantitative
3. Both
**Table 1 | Percentage of scientists who say that they engaged in the behaviour listed within the previous three years (n = 3,247)**

<table>
<thead>
<tr>
<th>Top ten behaviours</th>
<th>All</th>
<th>Mid-career</th>
<th>Early-career</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Falsifying or ‘cooking’ research data</td>
<td>0.3</td>
<td>0.2</td>
<td>0.5</td>
</tr>
<tr>
<td>2. Ignoring major aspects of human-subject requirements</td>
<td>0.3</td>
<td>0.3</td>
<td>0.4</td>
</tr>
<tr>
<td>3. Not properly disclosing involvement in firms whose products are based on one’s own research</td>
<td>0.3</td>
<td>0.4</td>
<td>0.3</td>
</tr>
<tr>
<td>4. Relationships with students, research subjects or clients that may be interpreted as questionable</td>
<td>1.4</td>
<td>1.3</td>
<td>1.4</td>
</tr>
<tr>
<td>5. Using another’s ideas without obtaining permission or giving due credit</td>
<td>1.4</td>
<td>1.7</td>
<td>1.0</td>
</tr>
<tr>
<td>6. Unauthorized use of confidential information in connection with one’s own research</td>
<td>1.7</td>
<td>2.4</td>
<td>0.8 ***</td>
</tr>
<tr>
<td>7. Failing to present data that contradict one’s own previous research</td>
<td>6.0</td>
<td>6.5</td>
<td>5.3</td>
</tr>
<tr>
<td>8. Circumventing certain minor aspects of human-subject requirements</td>
<td>7.6</td>
<td>9.0</td>
<td>6.0 **</td>
</tr>
<tr>
<td>9. Overlooking others’ use of flawed data or questionable interpretation of data</td>
<td>12.5</td>
<td>12.2</td>
<td>12.8</td>
</tr>
<tr>
<td>10. Changing the design, methodology or results of a study in response to pressure from a funding source</td>
<td>15.5</td>
<td>20.6</td>
<td>9.5 ***</td>
</tr>
</tbody>
</table>

**Other behaviours**

<table>
<thead>
<tr>
<th></th>
<th>All</th>
<th>Mid-career</th>
<th>Early-career</th>
</tr>
</thead>
<tbody>
<tr>
<td>11. Publishing the same data or results in two or more publications</td>
<td>4.7</td>
<td>5.9</td>
<td>3.4 **</td>
</tr>
<tr>
<td>12. Inappropriately assigning authorship credit</td>
<td>10.0</td>
<td>12.3</td>
<td>7.4 ***</td>
</tr>
<tr>
<td>13. Withholding details of methodology or results in papers or proposals</td>
<td>10.8</td>
<td>12.4</td>
<td>8.9 **</td>
</tr>
<tr>
<td>14. Using inadequate or inappropriate research designs</td>
<td>13.5</td>
<td>14.6</td>
<td>12.2</td>
</tr>
<tr>
<td>15. Dropping observations or data points from analyses based on a gut feeling that they were inaccurate</td>
<td>15.3</td>
<td>14.3</td>
<td>16.5</td>
</tr>
<tr>
<td>16. Inadequate record keeping related to research projects</td>
<td>27.5</td>
<td>27.7</td>
<td>27.3</td>
</tr>
</tbody>
</table>

Note: significance of χ² tests of differences between mid- and early-career scientists are noted by ** (P < 0.01) and *** (P < 0.001).

_Nature_ 435, 737-738 (9 June 2005) **Scientists behaving badly**
_Brian C. Martinson, Melissa S. Anderson & Raymond de Vries_
Have you begun record keeping for your research?

1. Yes
2. No

75% Yes
25% No
For only those who answered “Yes”. Recording Keeping in my research is adequate to enable later assessment of the integrity of the data and the resulting findings.

1. Strongly agree
2. Agree
3. Neutral
4. Disagree
5. Strongly disagree
Insuring Data Integrity

- UNDERSTAND.....the goals
- AGREE ON METHODS.....before research begins
- UNDERSTAND....how to carry out these methods
- RECORD ALL PROCEDURES IN A PERMANENT FORM. These data records should be maintained in their original and unaltered formats.
- ENSURE....your equipment works — VALIDATE!
EPIGEUM Module 3

- Data Interpretation and presentation
NSF Data Management Plan

NSF Data Sharing Policy

- Investigators are expected to share with other researchers, at no more than incremental cost and within a reasonable time, the primary data, samples, physical collections and other supporting materials created or gathered in the course of work under NSF grants. Grantees are expected to encourage and facilitate such sharing. See Award & Administration Guide (AAG) Chapter VI.D.4.

- NSF Data Management Plan Requirements

- Proposals submitted or due on or after January 18, 2011, must include a supplementary document of no more than two pages labeled “Data Management Plan”. This supplementary document should describe how the proposal will conform to NSF policy on the dissemination and sharing of research results. See Grant Proposal Guide (GPG) Chapter II.C.2.j for full policy implementation.
NSF Data Management Plan Contents

- **Products of the Research:** The types of data, samples, physical collections, software, curriculum materials, and other materials to be produced in the course of the project.

- **Data Formats:** The standards to be used for data and metadata format and content (where existing standards are absent or deemed inadequate, this should be documented along with any proposed solutions or remedies).

- **Access to Data and Data Sharing Practices and Policies:** Policies for access and sharing including provisions for appropriate protection of privacy, confidentiality, security, intellectual property, or other rights or requirements.

- **Policies for Re-Use, Re-Distribution, and Production of Derivatives.**

- **Archiving of Data:** Plans for archiving data, samples, and other research products, and for preservation of access to them.
Help with data at MSU

- **Michigan State University**
  MSU Libraries: Lifecycle Data Management Planning
  [http://www.lib.msu.edu/about/diginfo/ldmp.jsp](http://www.lib.msu.edu/about/diginfo/ldmp.jsp)

- VISIT THIS!
DATA SHARING

- Data sharing is the practice of making data used for scholarly research available to other investigators.

- Many funding agencies, institutions, and publication venues have policies regarding data sharing because transparency and openness are considered by many to be part of the scientific method.

What Data do you share?

- Large Data bases
- Microarray information
- Genetic Sequences
The NIH policy on data sharing applies:

- To the sharing of final research data for research purposes.
- To basic research, clinical studies, surveys, and other types of research supported by NIH. It applies to research that involves human subjects and laboratory research that does not involve human subjects. It is especially important to share unique data that cannot be readily replicated.
- To applicants seeking $500,000 or more in direct costs in any year of the proposed project period through grants, cooperative agreements, or contracts.
- To research applications submitted beginning October 1, 2003.
Journal Open-Data Policies

- [http://oad.simmons.edu/oadwiki/Journal_open-data_policies](http://oad.simmons.edu/oadwiki/Journal_open-data_policies)

This is a list of journals with data-sharing mandates for their published articles. For example:

- **African Journal of Ecology**
  - Data that is integral to the paper must be made available in such a way as to enable readers to replicate, verify and build upon the conclusions published in the paper. Any restriction on the availability of this data must be disclosed at the time of submission.

- **Evolution**
  - Require authors to submit DNA sequence data to GenBank and phylogenetic data to TreeBase.
Limitations & Restrictions on Sharing of Data

- Health Insurance Portability & Protection Act (HIPAA)
- Sensitive but Unclassified Data
- Classified & Restricted Research Activities
- Intellectual Property Protections
- Ethical considerations
Why data-sharing policies matter

Alan E. Guttmacher\textsuperscript{a,1}, Elizabeth G. Nabel\textsuperscript{b}, and Francis S. Collins\textsuperscript{c}

\textsuperscript{a}National Human Genome Research Institute, National Institutes of Health, Bethesda, MD 20892; \textsuperscript{b}National Heart, Lung, and Blood Institute, National Institutes of Health, Bethesda, MD 20892; and \textsuperscript{c}National Institutes of Health, Bethesda, MD 20892

A recent breach by a recipient investigator of the Data Use Certification led to the on-line publication by PNAS of a manuscript that should never even have been submitted (2). While both PNAS and the NIH will deal with this specific breach, it is the wider research community that must police itself and prevent inappropriate publication in the future.
...our editors became aware that Dr. Zhang had signed a Data Use Certification indicating his agreement to comply with the NIH Genome-Wide Association Studies Policy for Data Sharing, which applies to the Gene Environment Association (GENEVA) studies, of which the Study of Addiction, Genetics and Environment (SAGE) is a part. Under the policy, investigators agree not to submit findings of the SAGE dataset(s) for publication until September 23, 2009. The *PNAS* publication clearly violates the SAGE embargo, and the authors agreed to retract their work in *PNAS* on September 9, 2009.
Research/Scholarly Integrity Resources

- NAS, Ensuring the Integrity, Accessibility, and Stewardship of Research Data in the Digital Age

- NIH Data Sharing Policy and Implementation Guidance

- UM, Research Data Management and Publishing Support (NSF Plans)

- MN, Funding Agency and Data Management Guidelines
  - [http://www.lib.umn.edu/datamanagement/funding](http://www.lib.umn.edu/datamanagement/funding)

- MSU, Lifecycle Data Management Planning
  - [http://www.lib.msu.edu/about/diginfo/ldmp.jsp](http://www.lib.msu.edu/about/diginfo/ldmp.jsp)
Discuss with your research integrity consultant ways that it is appropriate to manipulate data and research/scholarly results in your discipline. Also discuss examples of manipulating data and research/scholarly results in your discipline that would NOT be proper.
On your Sheet

What is one form of data (sample, file, image) that you know will be essential for your thesis/postdoctoral work?
NEXT WORKSHOP

- Conflict of Interest, Peer Review, & Export Control
- Wednesday, January 13, 2016
  - [http://grad.msu.edu/rcr/integrity.aspx](http://grad.msu.edu/rcr/integrity.aspx)
- Workshop Series Syllabus
  - [http://grad.msu.edu/rcr/docs/syllabus.pdf](http://grad.msu.edu/rcr/docs/syllabus.pdf)