Responsible Conduct of Research, Scholarship, and Creative Activities

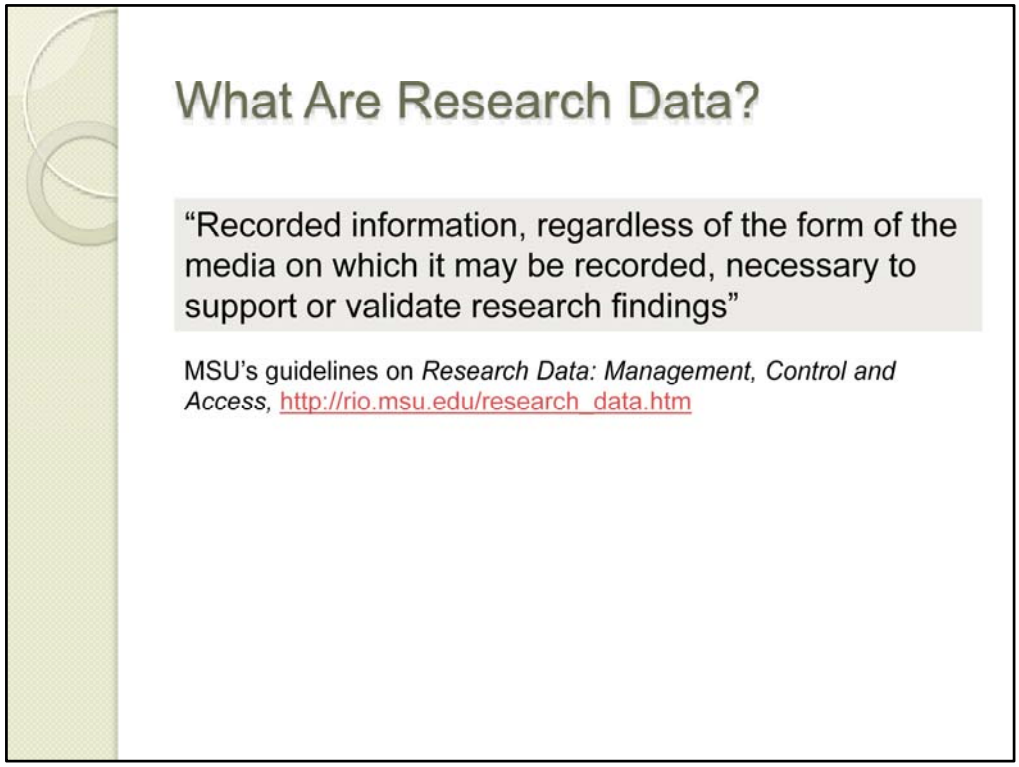
Management of Research Data

Objectives

- Understand what is meant by: (a) research data; (b) control, access, and ownership of research data; (c) material transfer agreements, and (d) export controls
- How do researchers in your discipline maintain the integrity and security of research data?
- What is the plan for "disaster recovery" of research data in your discipline?
- Describe the extent to which students have access and ownership of research data.
- Where should MSU faculty, students, and staff seek advice about disputes related to data management?

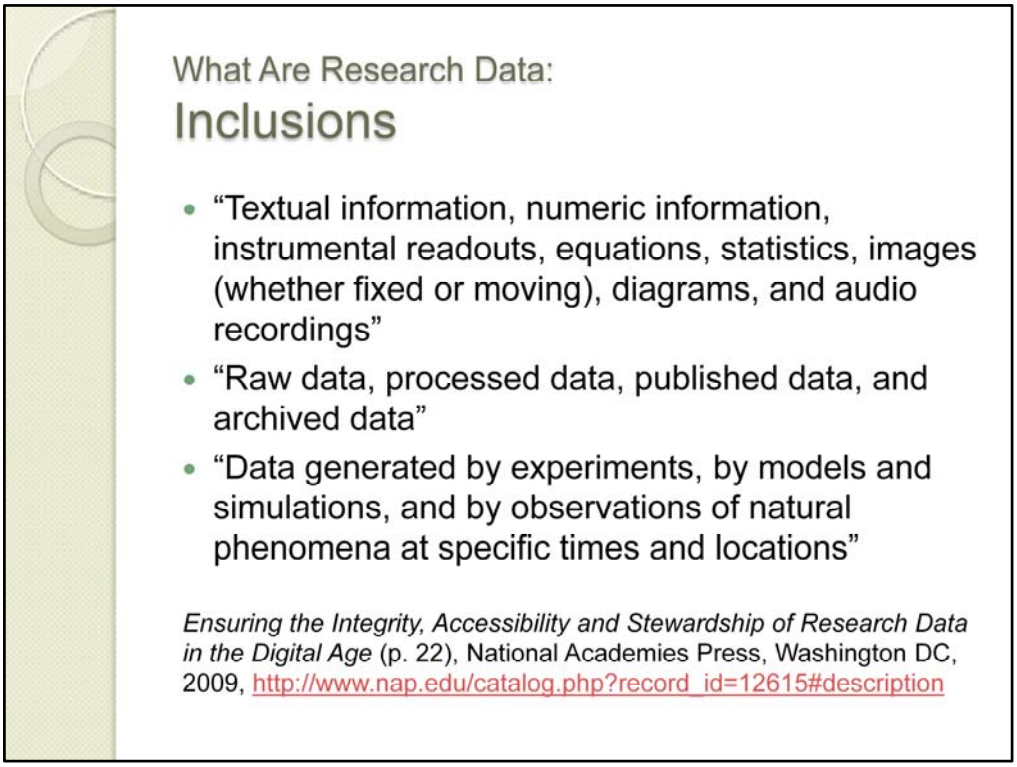
Part 1: Introduction

- What are research data?
- Research data in your discipline
- Management of research data



The MSU definition is very similar to the operational definition provided by the National Academies (National Academy of Science, National Academy of Engineering, and Institute of Medicine) in their text, *Ensuring the Integrity, Accessibility and Stewardship of Research Data in the Digital Age* (p.22), National Academies Press, Washington, DC, 2009, http://www.nap.edu/catalog.php?record_id=12615#description .

National Academies definition:
"Information used in scientific, engineering, and medical research as inputs to general research conclusions"



Note: There is no universal agreement about what constitutes research data.

The definition of research data from the MSU guidelines (http://rio.msu.edu/research_data.htm) includes "laboratory notebooks, as well as x-ray film, photographs, negatives and slides, print outs, video and audio tape, computers and computer data storage devices, and synthetic compounds, organisms, cell lines, viruses, cell products, cloned coordinates, plants, animals and spectroscope data, however recorded or preserved." The reader should understand that MSU has guidelines, but not policy, related to research data.

As noted on subsequent slides, some of the items included in the MSU guidelines are specifically excluded in the definition set forth by the National Academies (*Ensuring the Integrity, Accessibility and Stewardship of Research Data in the Digital Age*, National Academies Press, Washington, DC, 2009, http://www.nap.edu/catalog.php?record_id=12615#description).

What Are Research Data:
Inclusions, *continued*

- "Data gathered specifically for research as well as information gathered for other purposes that is then used for research"
- "Data stored on a wide variety of media, including magnetic and optical media"

Ensuring the Integrity, Accessibility and Stewardship of Research Data in the Digital Age (p. 22), National Academies Press, Washington DC, 2009, http://www.nap.edu/catalog.php?record_id=12615#description

What Are Research Data:

Exclusions

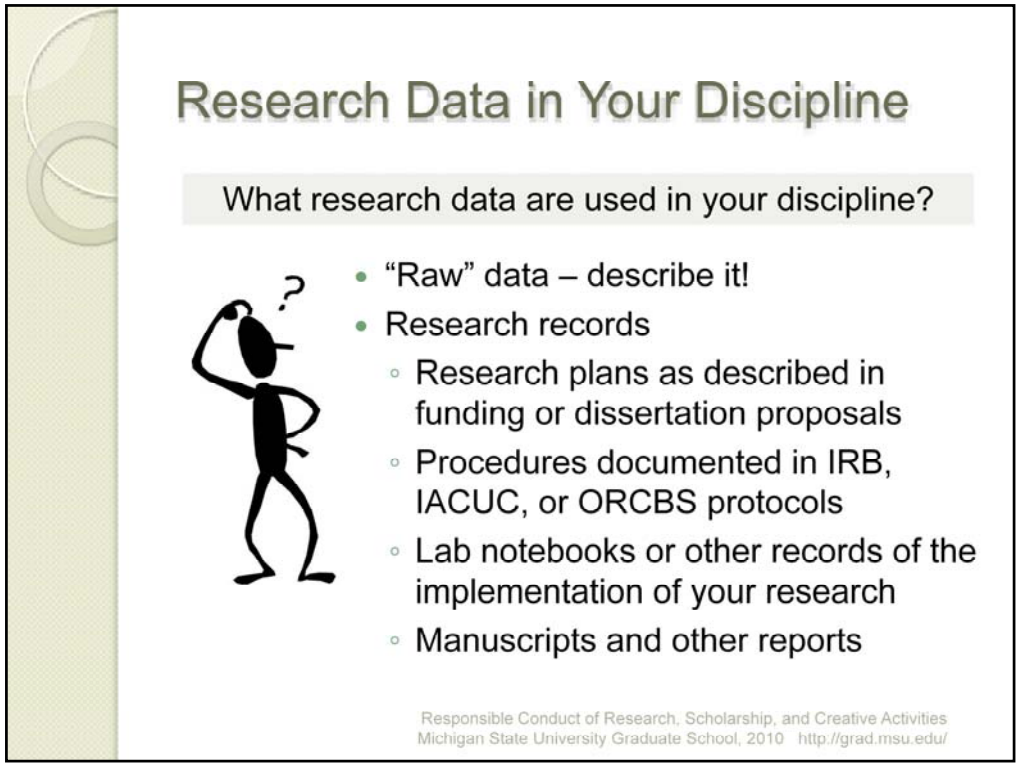
- "Physical objects (including living organisms) and other materials used in research such as biological reagents or the devices, instruments, or computers that generate experimental or observational data"
  - Note that written, numeric, or visual descriptions of physical objects do constitute data
- "Information that can be important in research but is not used to generate research conclusions including interpretive statements, or matters of personal judgment …"

Ensuring the Integrity, Accessibility and Stewardship of Research Data in the Digital Age (p. 23), National Academies Press, Washington DC, 2009, http://www.nap.edu/catalog.php?record_id=12615#description

What Are Metadata?

- Investigators should consider appropriate means of developing and storing *metadata* as part of the overall research record
  - The term *metadata* refers to descriptions of "data content, context, structure, interrelationships, and provenance (information on history and origins)"
  - Metadata "add relevance and purpose to data, and enable the identification of similar data in different data collections"

Ensuring the Integrity, Accessibility and Stewardship of Research Data in the Digital Age (p. 24), National Academies Press, Washington DC, 2009, http://www.nap.edu/catalog.php?record_id=12615#description

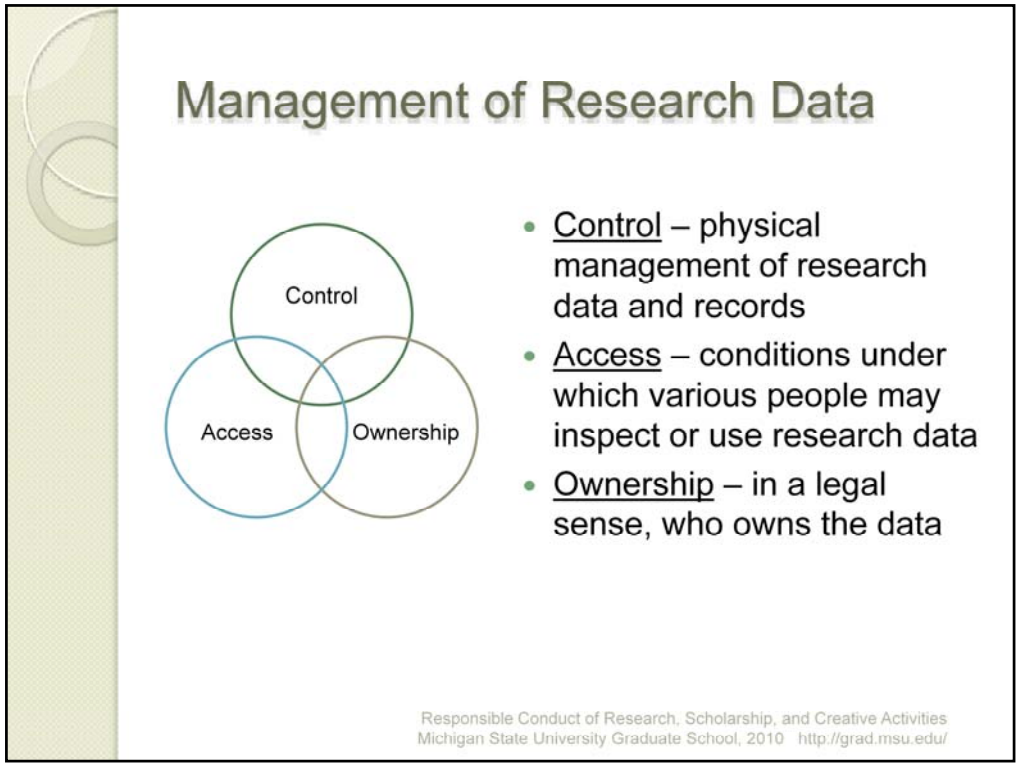


The term "raw data" refers to research data in its original form before entry into computer files or other forms of storage.

Make a list of all research data that you do (or might) use in your research. The definition of research data on the previous slide should help you to think about possibilities.

Refer to your list as you continue studying this presentation. You will learn more if you apply the content of this presentation to your own discipline.

IRB = Institutional Review Board. Reviews proposals to conduct research involving human subjects.
IACUC = Institutional Animal Care and Use Committee. Reviews proposals to conduct research involving animals.
ORCBS = Office of Radiation, Chemical, and Biological Safety. Monitors use of hazardous substances in research.



Did you know …

- Funded research belongs to the university.
- MSU technically delegates management of the research project to the principle investigator (PI).
- Thus, MSU has a definite stake in the conduct of research. In addition, MSU has responsibility to support researchers via services such as contracts and grants, intellectual property, IRB, and other offices.

The majority of this presentation is organized around the principles of control, access, and ownership

Management of Research Data:

Data Integrity Principle

"Ensuring the integrity of research data is essential for advancing scientific, engineering, and medical knowledge and for maintaining public trust in the research enterprise. Although other stakeholders in the research enterprise have important roles to play, researchers themselves are ultimately responsible for ensuring the integrity of research data."

From *Ensuring the Integrity, Accessibility, and Stewardship of Research Data in the Digital Age* (p. 4), National Academies Press, Washington, DC, 2009.

Management of Research Data:

Data Access and Sharing Principle

"Research data, methods, and other information integral to publicly reported results should be publicly accessible."

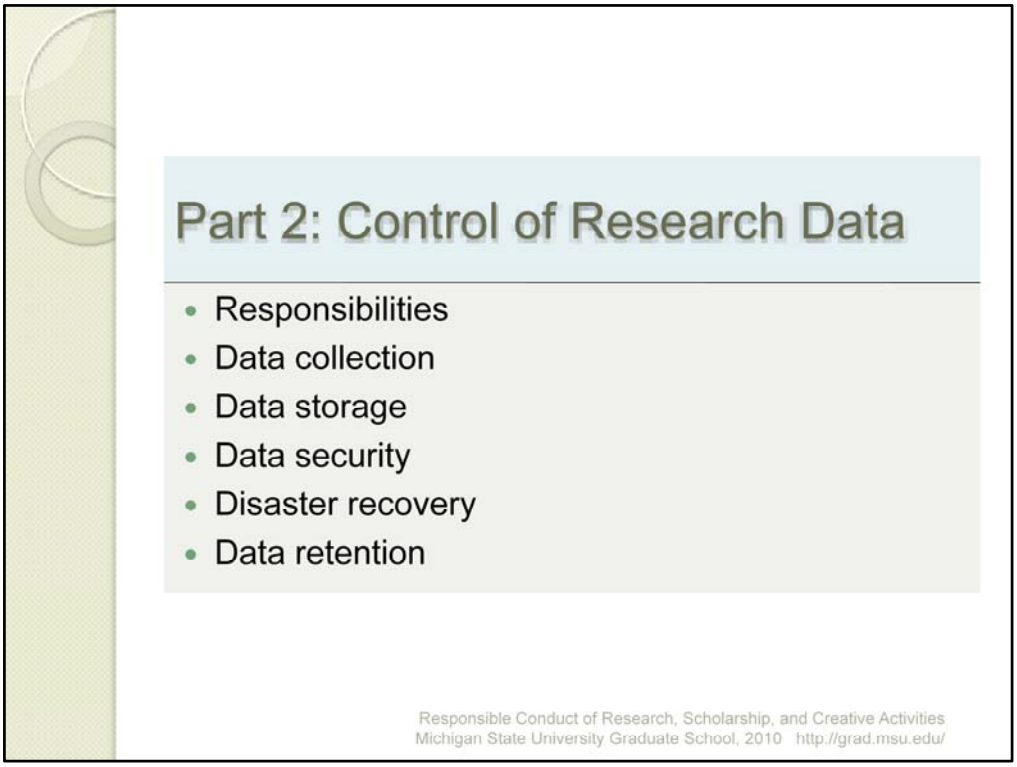
From *Ensuring the Integrity, Accessibility, and Stewardship of Research Data in the Digital Age* (p. 6), National Academies Press, Washington, DC, 2009.

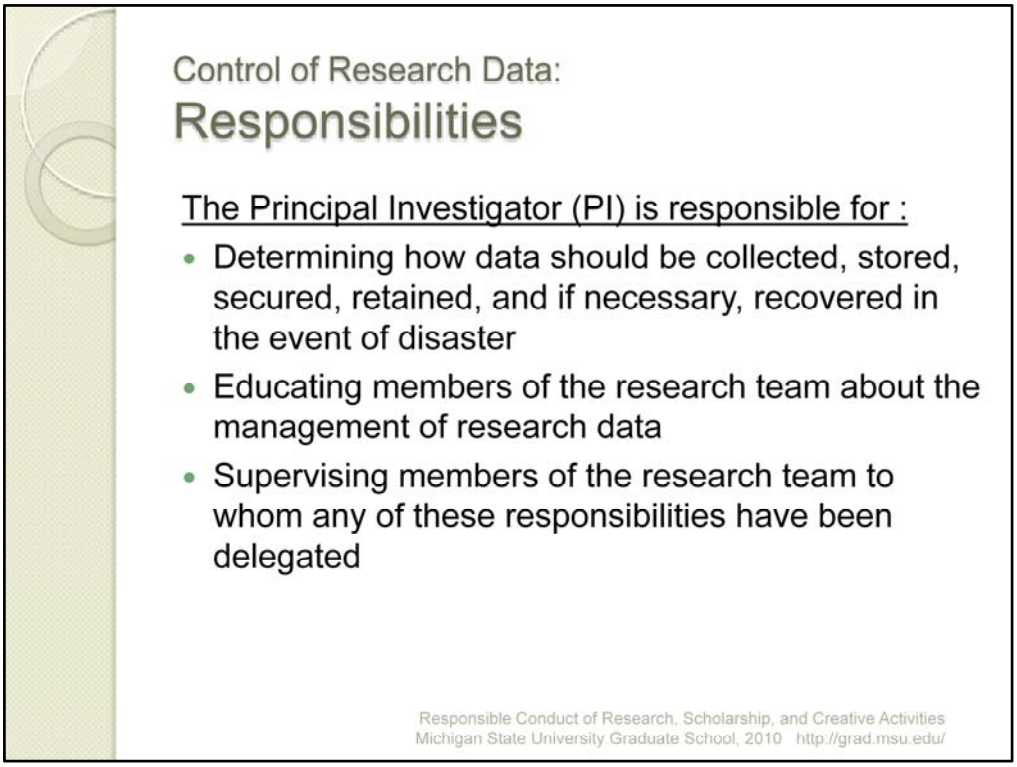
Management of Research Data:

Data Stewardship Principle

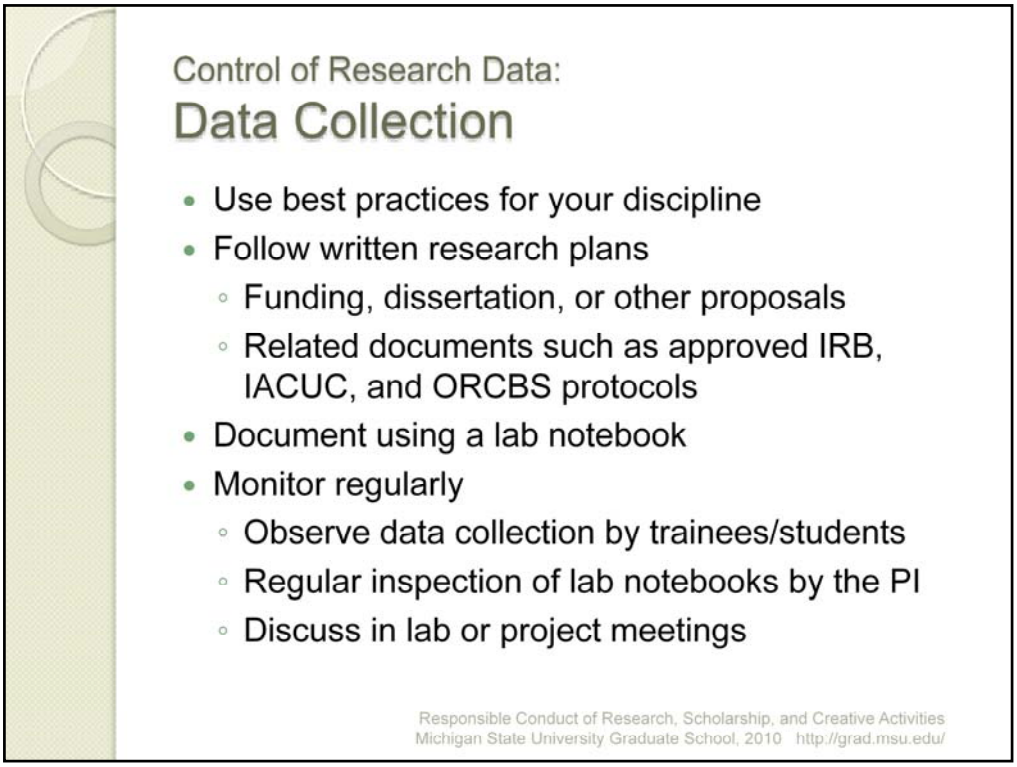
"Research data should be retained to serve future uses. Data that may have long-term value should be documented, referenced, and indexed so that others can find and use them accurately and appropriately."

From *Ensuring the Integrity, Accessibility, and Stewardship of Research Data in the Digital Age* (p. 8), National Academies Press, Washington, DC, 2009.


Part 2: Control of Research Data
Responsibilities
Data collection
Data storage
Data security
Disaster recovery
Data retention
Responsible Conduct of Research, Scholarship, and Creative Activities
Michigan State University Graduate School, 2010 http://grad.msu.edu/



MSU guidelines: "The PI is the custodian of the primary data, unless agreed on in writing otherwise, and is responsible for the collection, management, and retention of research data. The PI should adopt an orderly system of data organization and should communicate the chosen system to all members of a research group and to the appropriate administrative personnel, where applicable." (*Research Data: Management, Control, and Access,* http://rio.msu.edu/research_data.htm)



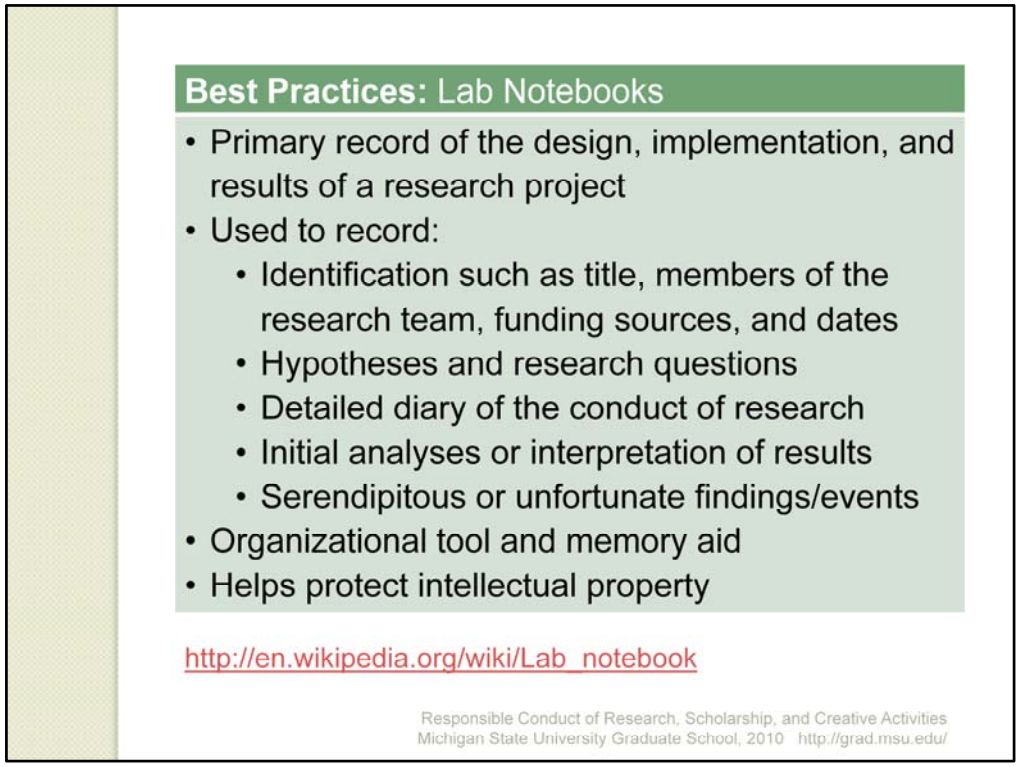
Use best practices: Conduct a comprehensive review of literature to determine the most accurate, reliable, and objective methods. Members of the research team should be trained for their responsibilities. Where appropriate, members of the research team should be certified to use data collection equipment and materials.

Follow written research plan: The PI should make certain that every member of the research team has a complete understanding of the data collection plan as documented in research proposal, as well as any approved IRB, IACUC, and ORCBS protocols.

- IRB = Institutional Review Board (http://www.humanresearch.msu.edu). Reviews proposals to conduct research involving human subjects.
- IACUC = Institutional Animal Care and Use Committee (http://www.vprgs.msu.edu/animal_use_care). Reviews proposals to conduct research involving animals.
- ORCBS = Office of Radiation, Chemical, and Biological Safety (http://www.orcbs.msu.edu/). Monitors use of hazardous substances in research.

Document using a lab notebook: Lab notebooks are comprehensive diaries of the implementation of a research projects. General guidelines for writing lab notebooks can be found using internet search engines. Discipline-specific guidelines for writing lab notebooks exist in some fields of study. Students and trainees should ask their mentors about preferred methods.

Monitor regularly: The PI is responsible for either collecting the data, or monitoring members of the research team who do collect the data. Although this responsibility may be delegated to some extent, in the final analysis, the PI is responsible for the integrity of the data as well as compliance with written research plans and related documents. The PI's responsibilities include regular inspection of lab notebooks.



General requirements:

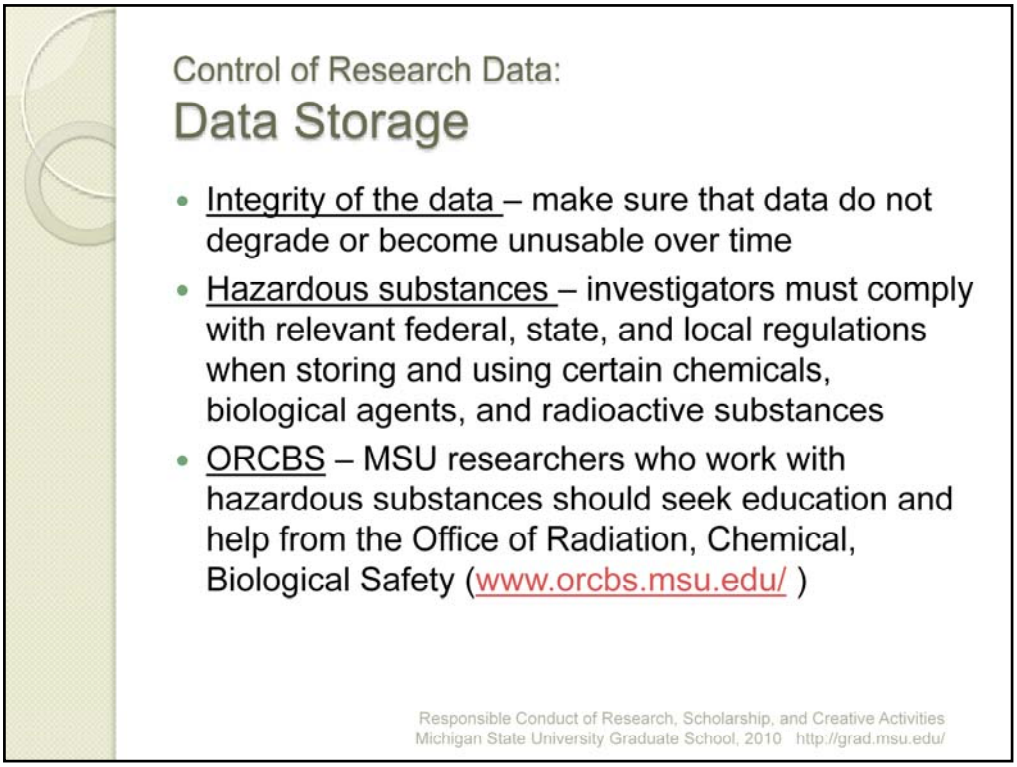
- Use a bound notebook with numbered pages and do not remove pages
- Label and date the notebooks
- Date and sign/initial each page and entry
- Have a witness sign/initial each page and entry
- Make entries in ink and line-out and initial changes using a different color ink
- Tape or glue evidence into the notebook as needed

Lab notebook entries:

- Title of the study
- PI and research team
- Start and end dates
- Hypotheses/goals
- Subjects and assignment to groups
- Hazardous materials
- Detailed diary of implementation of the study
- Techniques and statistical approaches that differ from the methodology notebook
- Timeline
- Raw data or instructions for locating raw data
- Conclusions drawn from study

Sources:

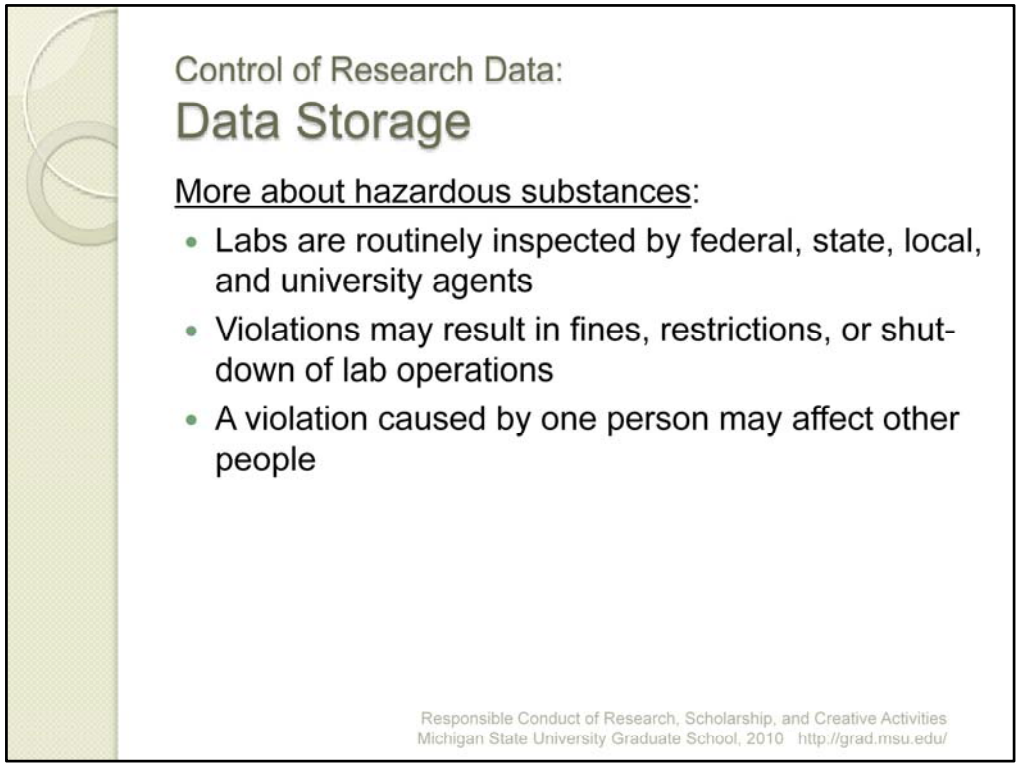
- Howard M. Kanare. (1985). *Writing the Laboratory Notebook*. Washington DC: American Chemical Society.
- *Laboratory Notebook*. (n.d.). U.S. Office of Research Integrity, http://ori.dhhs.gov/education/products/wsu/data_lab.html.
- Use an internet search engine and the key words “writing laboratory notebook” to locate additional guidelines.



Integrity. Methods of insuring data integrity depend upon the nature of the data. For example, electronic data should be kept on high-quality computer storage media. Certain biological samples must be stored in freezers maintained at very low temperatures. And historical documents should be preserved on archival paper in low-humidity settings. Researchers must understand the nature of data used in their disciplines, as well as appropriate methods of storing those data.

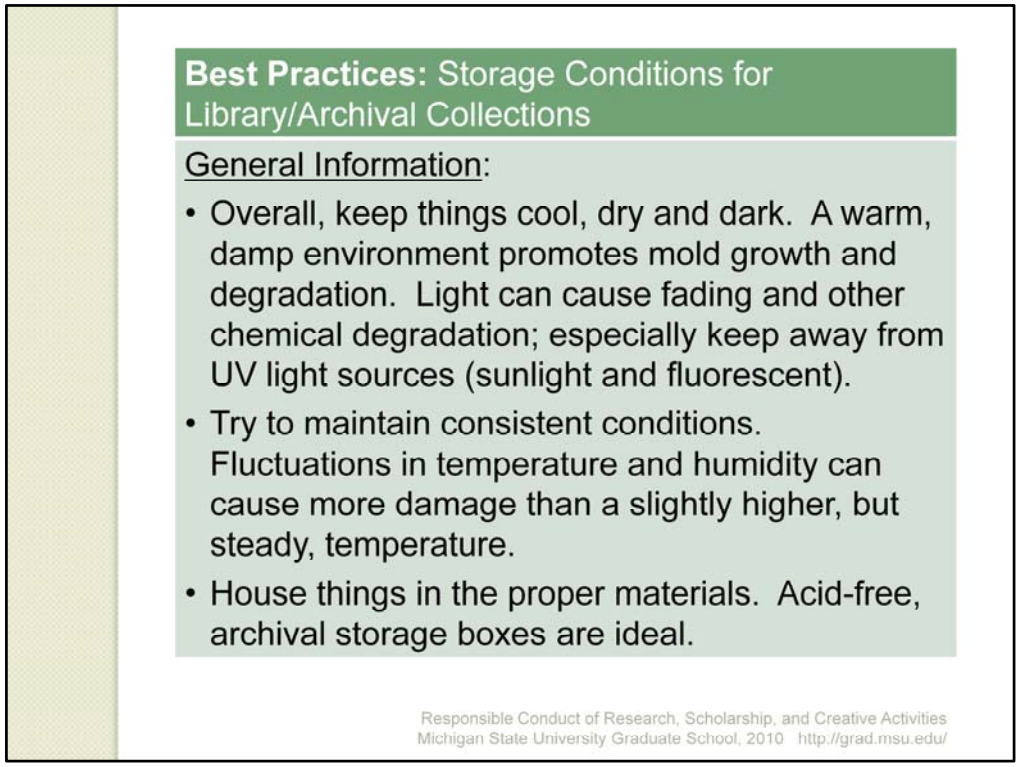
Hazardous substances – Two recent federal laws focus on national security issues related to possession and use of select hazardous substances.

- The 2001 Patriot Act makes it a crime to knowingly possess any biological pathogen, toxin, or delivery system that cannot be "reasonably justified by a prophylactic, protective, bona fide research, or other peaceful purpose." The law also excludes from access to dangerous pathogens several categories of people, including nonresident aliens from countries on the State Department's list of nations that support terrorism. That exclusion is applied without exception or right of appeal.
- The 2002 Bioterrorism Act, also known as the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, was passed in the wake of the anthrax attacks. This law mandates the regulation of all American domestic facilities that possess, work with, or transfer one or more "select agents" on a list of 82 human, animal, and plant pathogens and toxins. Such facilities must register with the Centers for Disease Control for human pathogens, or the Department of Agriculture's Animal and Plant Health Inspection Service for plant and animal pathogens. The registered institutions must implement measures to prevent terrorists from gaining access to the select agents in their possession, such as conducting risk assessments and improving physical security and pathogen accounting procedures. In addition, the roughly 9,000 American scientists seeking to work with listed agents must undergo an FBI security-risk-assessment screening against criminal, immigration, terrorism, and other national-security.
- Source: Jonathan B. Tucker, *Research on biodefense can get generous funds, but with strings attached*, *The Chronicle Review*, Volume 50, Issue 26, Page B10, 3/5/04. Available at http://chronicle.com



A violation caused by one person may affect other people

- The inappropriate use of hazardous substances may contaminate research samples throughout the lab
- The health and safety of people who work in the lab may be compromised
- If the lab is shut-down, all research projects conducted in that lab are affected
- If funding is lost because of violations, research projects may be cancelled and graduate assistantships may be terminated



Storage Conditions for Library/Archival Collections
More information available at the American Institute for Conservation (AIC) website: <http://www.conservation-us.org/> or contact the Wallace Conservation Lab at MSU Libraries <http://www2.lib.msu.edu/preservation/wallacelab.jsp>.

Paper, books, and photos:

- Store paper and books below 22°C (72°F) and 35% relative humidity
- Store photographs at 18°C (64°F) and 30%-40% relative humidity
- More information at Library of Congress Collections Care and Conservation web site <http://www.loc.gov/preserv/pubscare.html>

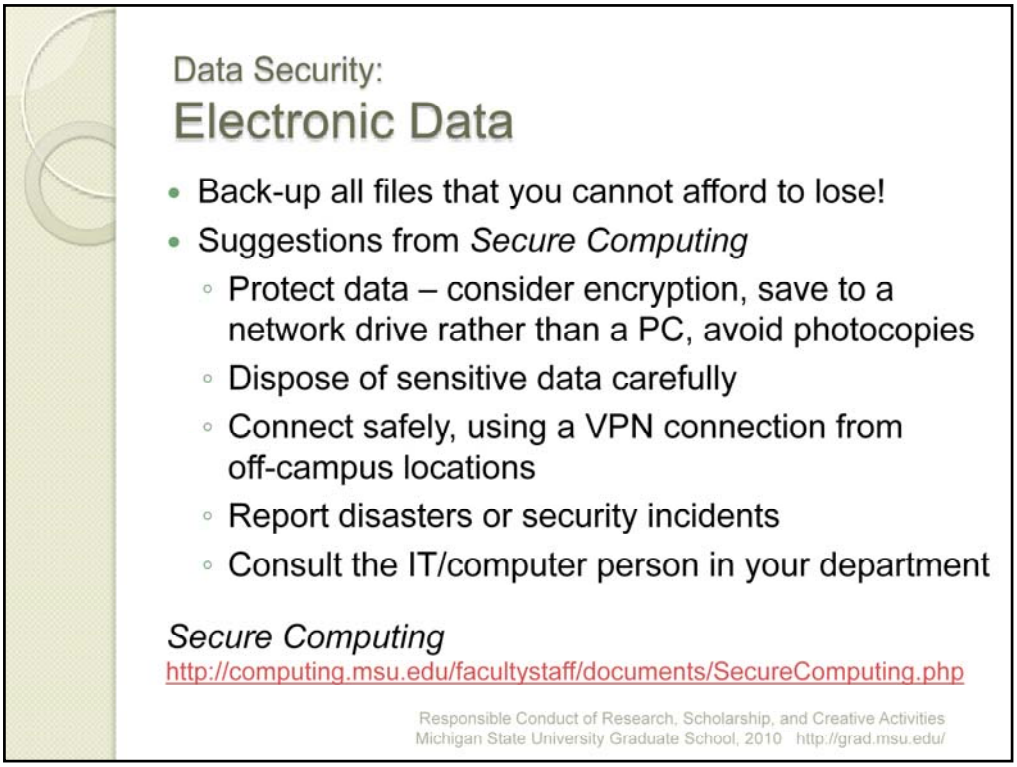
Computer media:

- Store magnetic media (video and audio cassettes, computer disks) at 20°C (68°F) and 40% relative humidity – more information at http://www.clir.org/pubs/reports/pub54/
- Store optical media (CDs) at 18°-23°C (65°-75°F) and 30%-50% relative humidity
- All magnetic and optical media have a limited life and must be migrated on a regular schedule

Control of Research Data:

Data Security

- Avoid unauthorized access, use, theft, and vandalism of research data
- Data security depends on:
  - Storing research data in safe locations – *covered in next three slides*
  - Limiting access to authorized persons – *covered in the "Data Access" section of this presentation*

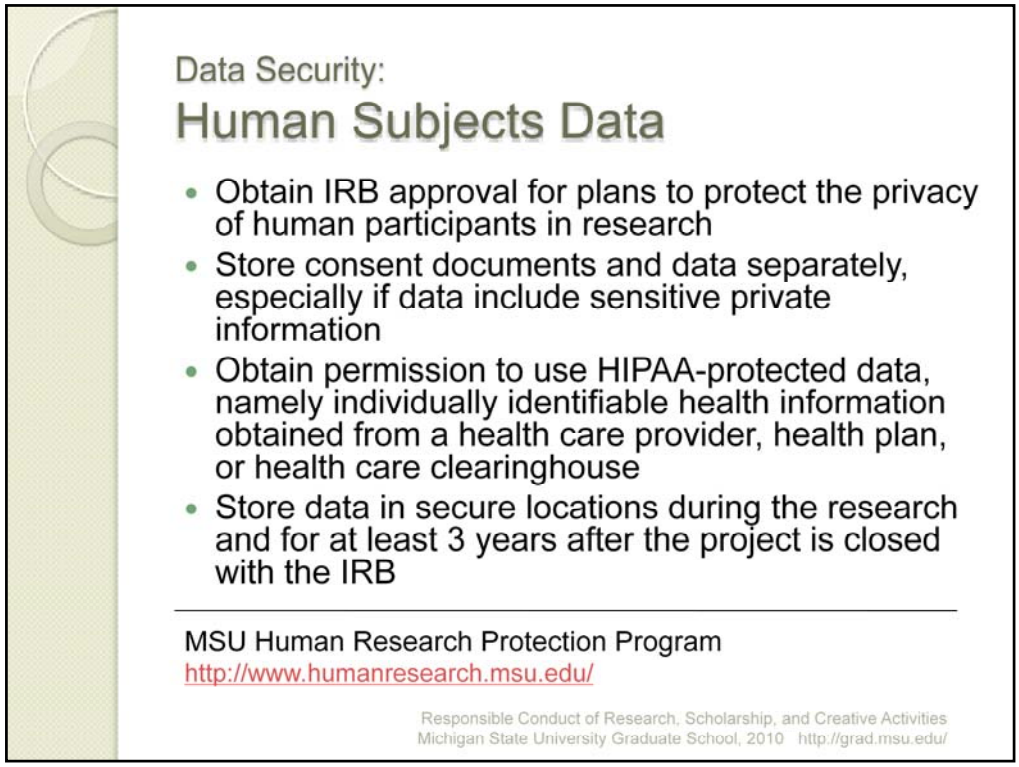


The following information is from *Secure Computing* (http://computing.msu.edu/facultystaff/documents/SecureComputing.php)

- Protect data: (a) treat all sensitive data as a highly valuable asset and minimize the chance that it is released to unauthorized users; (b) identify sensitive data inputs, location, and sensitivity; (c) do not use Social Security numbers as an identifier; (d) encrypt private data sent across the network; (e) save sensitive data files to a network drive, not a personal computer; (f) restrict access to sensitive data to those who "need to know"; (g) avoid copies; and (h) get rid of data no longer needed.
- Dispose of sensitive data carefully: (a) only store necessary data; (b) shred papers containing sensitive data; (c) follow the *Best Practices in Disposal of Computers and Electronic Storage Media* at lct.msu.edu/best practices; and (d) sanitize hard drives of disposed computers to remove sensitive data.
- Connect safely: (a) use only MSU-approved networks and wireless access points; (b) do not e-mail private data, as messages can be intercepted; (c) use a Virtual Private Network (VPN) when off campus for a secure connection (vpn.msu.edu); and (d) find out more about university guidelines regarding protecting sensitive data at computing.msu.edu/msd. VPN stands for "Virtual Private Networking". Learn more at http://computing.msu.edu/facultystaff/documents/RemoteAccess.php. VPN provides MSU faculty and students with secure access to the MSU network (including stored research data) from anywhere in the world. VPN access also provides the user with entry to restricted services, such as library databases.

The following information is from Keep it Safe (http://computing.msu.edu/secureIT):

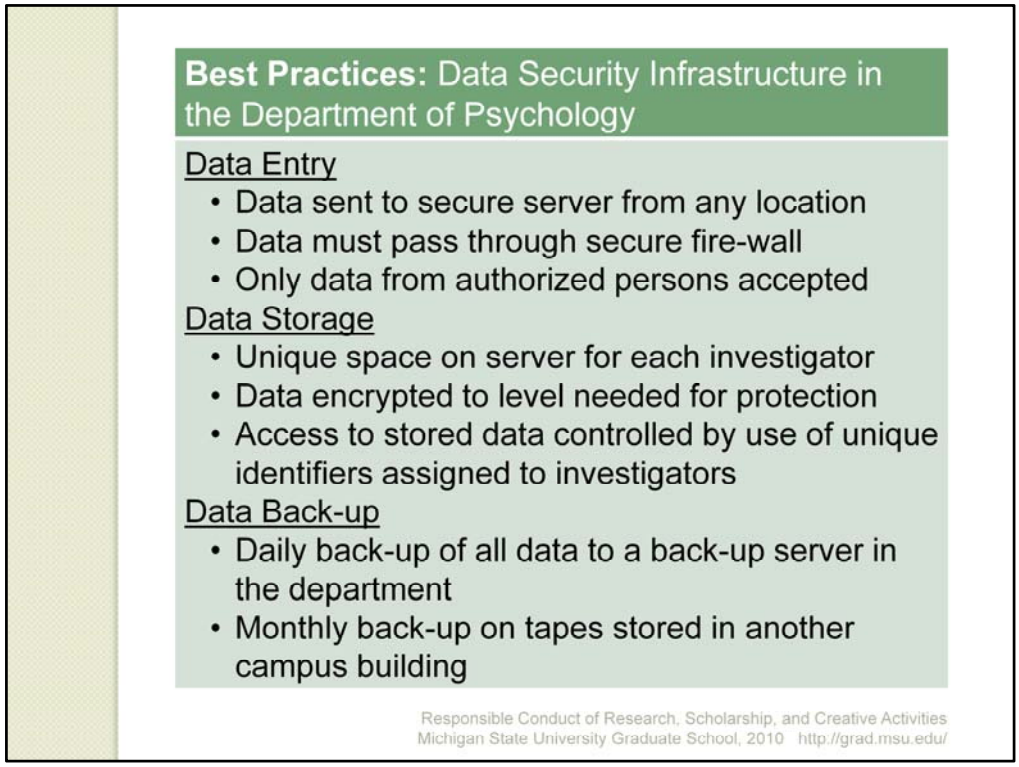
- Safeguard passwords: use strong passwords and keep the information confidential.
- Protect personal information: do not share personal information via email, and encrypt private data sent across networks or stored on a personal computer.
- Always use anti-virus and anti-spyware software: such software protects against viruses, worms, and malware.
- Turn on a personal firewall: block unwanted messages before they reach your computer.
- Apply software updates: updates often include security updates.



IRB refers to Institutional Review Board. MSU has three IRBs. Information for BIRB, SIRB, and CRIRB can be located at http://www.humanresearch.msu.edu/.

- BIRB – Biomedical and Health IRB
- SIRB – Social Science/Behavioral/Education IRB
- CRIRB – Community Research IRB

Go to http://www.humanresearch.msu.edu/hipaa.html for more information about the research implications of HIPAA, the Health Insurance Portability and Accountability Act



The data security infrastructure in the Department of Psychology is maintained by an information technology (IT) professional.

More information about data entry:

- Data may be entered on any computer on or off campus.
- Data are not stored on these "peripheral" computers
- Data are sent to a secure server maintained by the Department of Psychology
- Data must pass through a secure fire-wall with password protection
- An access control list (ACL) assures that data can be entered on the department server only by authorized persons

More information about data storage:

- The department server has a dedicated section for research data and another dedicated section for other faculty uses (e.g., course materials, committee work, department documents)
- Investigators have allocated space in the research section for each research project. More than one member of the research team may access the research project data if authorized.

More information about data back-up:

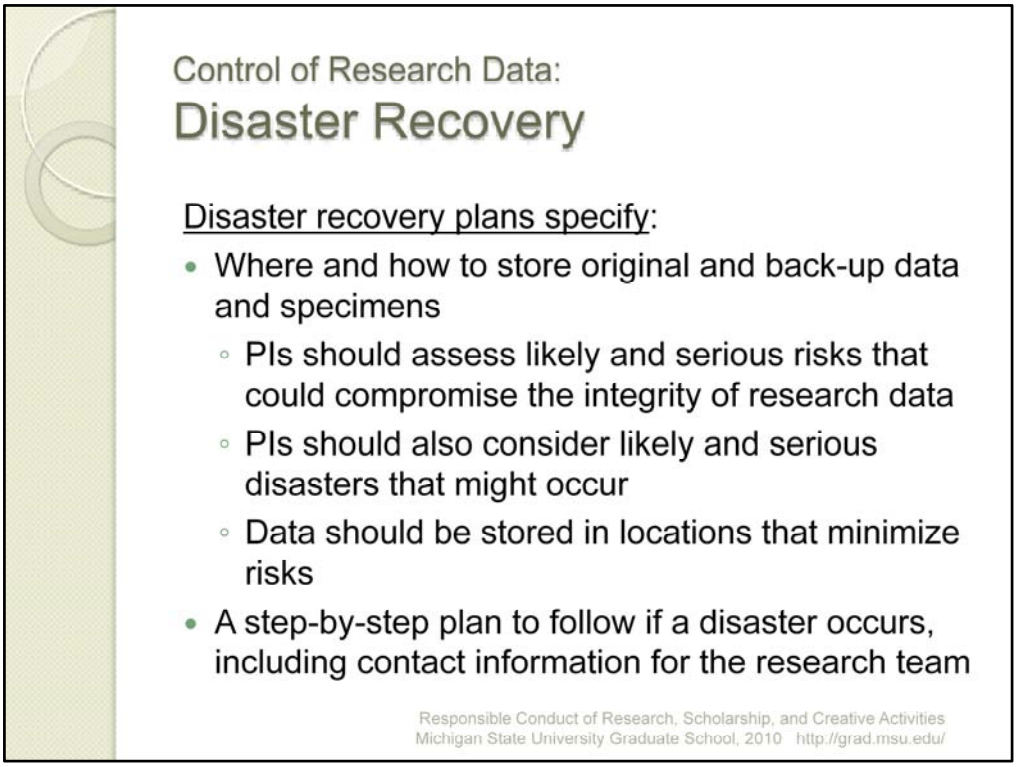
- The location of the tape back-ups is secret!

Control of Research Data:

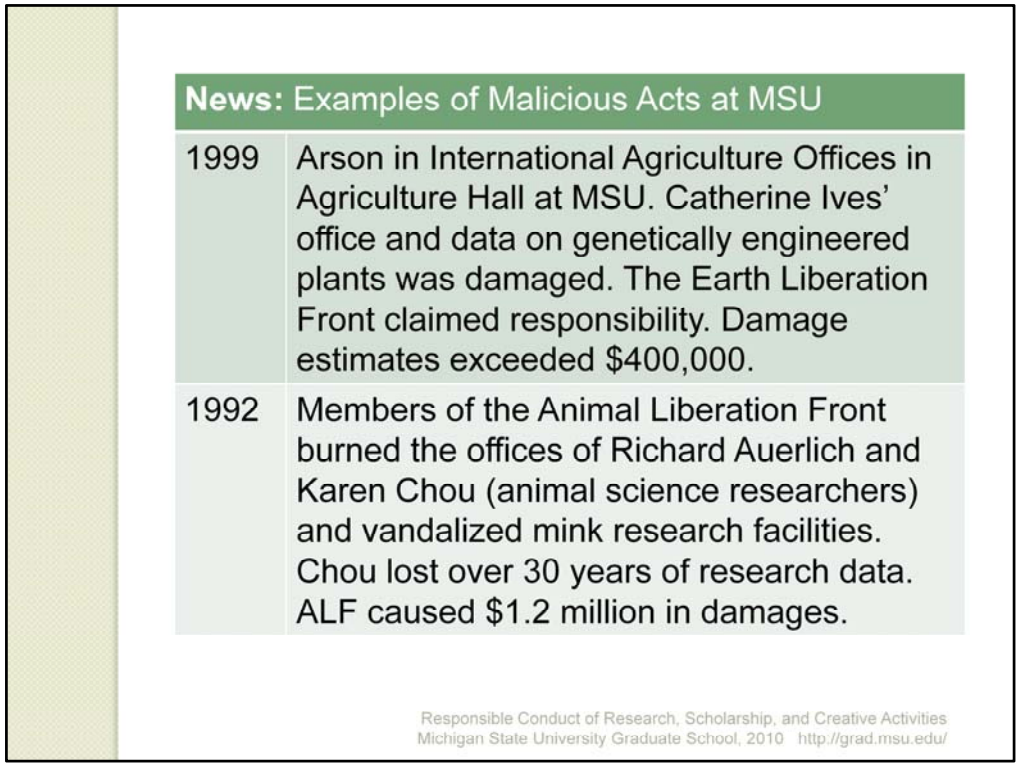
Disaster Recovery

Disasters include but are not limited to:

- Common events such as a computer “crash” or hard drive failure
- Accidents such as a broken water pipe or equipment malfunctions, including storage freezers or growth chambers
- Weather events such as tornados, floods, or earthquakes
- Malicious acts such as cyber attacks/hacking, arson, or vandalism



Back-up copies of electronic data may suffice in some cases, especially if the back-up copies are kept in a different office or building. Regular inspection of research equipment and facilities is essential. Alternate power supplies (e.g., back-up generator) may be needed in some cases. In general, more elaborate disaster recovery plans are needed the more sensitive or unique the data.



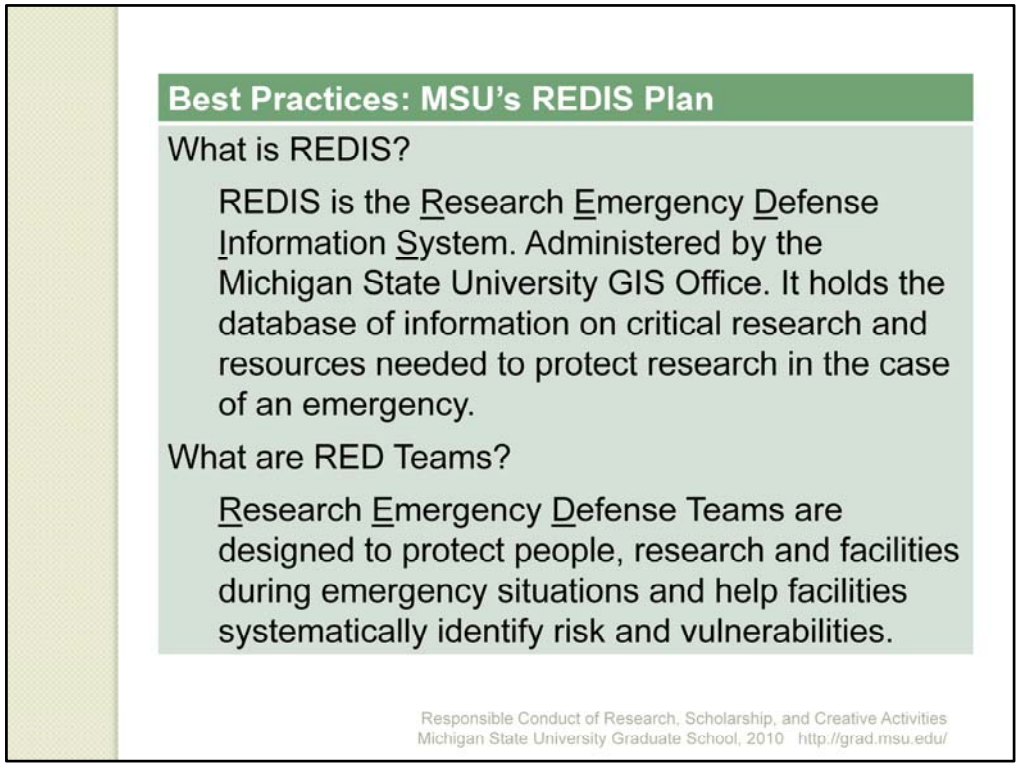
More information about the Agriculture Hall arson:

- K. Kirby. (n.d.). *Activist Activities and our Response.* http://www.appa.org/FacilitiesManager/articleDetail.cfm?ItemNumber=478
- *Environmental Group Claims Responsibility for Arson,* 1/24/00. http://www.canoe.ca/AllAboutCanoesNewsJan00/000124_fire.html
- http://special.news.msu.edu/ag_hall/index.php
- http://news.msu.edu/staff-faculty/NBarchivePDFS/Vol39/MSUNB_2008-03-27.pdf
- http://www.animalliberationfront.com/ALFront/Premise_History/1999_Chronicle_of_Direct_Actions.htm

More information about the animal science terrorism:

- http://www.the-scientist.com/yr1995/sept/notebk_950904.html

News: Other Disasters	
2009	Hacker taps into University of Alabama computer system exposing lab records
2008	Floods at the University of Iowa close buildings, interrupt research, and destroy some research data
2005	Hurricane Katrina ravaged research facilities at universities in Louisiana and neighboring states
1994	Earthquake devastated most of the Cal State Northridge campus



What is REDIS?

REDIS is the Research Emergency Defense Information System. Administered by the Michigan State University GIS Office, it holds the database of information on critical research and resources needed to protect research in the case of an emergency.

What are Red Teams?

Research Emergency Defense Teams (RED Teams) are designed to protect people, research and facilities during emergency situations and help facilities systematically identify risk and vulnerabilities. They also facilitate collaboration between key emergency personnel and the University, research areas and critical function areas.

RED Teams are comprised of a team leader and representatives from ORCBS, MSU Police Department, East Lansing Fire Department, Emergency Action Team Coordinators (yellow hats), Department Safety Committees, Department Chair, MSU Physical Plant and individual Building Contact teams.

Sample Excerpt from a REDIS Building Report

Building X

FIRST FLOOR

Room **xx**

Lecture cabinet with PC and other electronic equipment (Computer equipment/Process Computers)

Description: Portable multi-functional lectionary with PC, speakers, etc. for presentations

Location: South wall of Room xx

Room **yy**

Room yy is for flammable storage (Chemicals/Flammables (over 10 gallons))

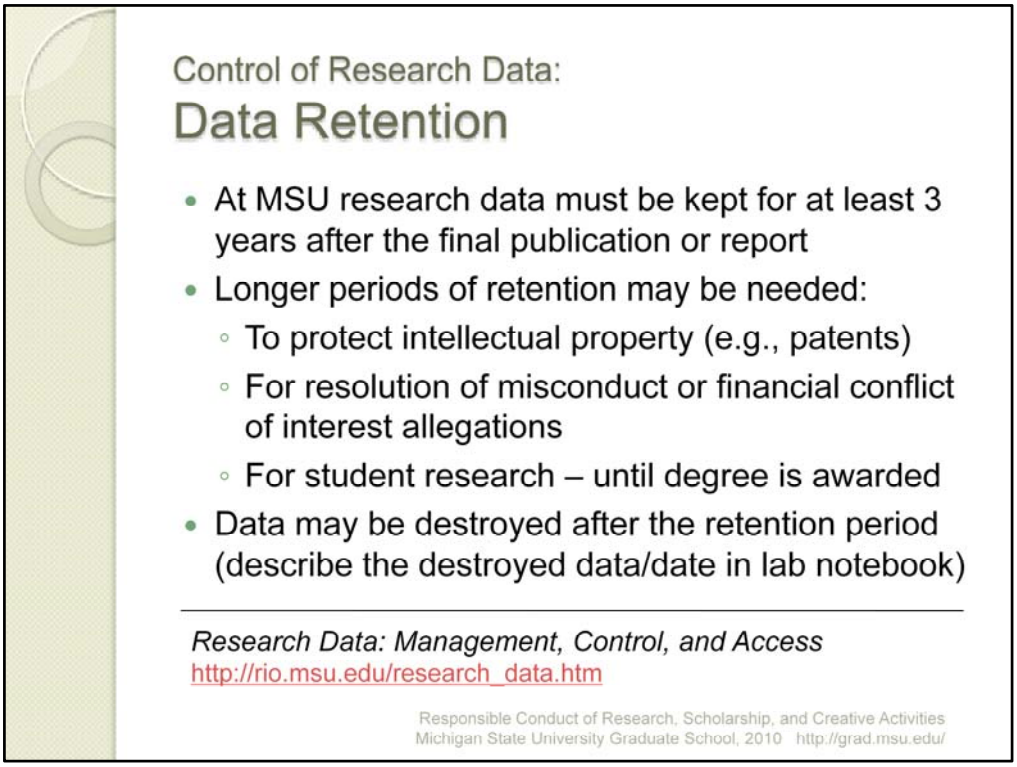
Description: All 4L bottles of flammables, acids and bases are stored in their shipping containers. The stock is for supplying the XYZ Research Store in Room yy. Chemicals stored include Ether (1L size), Alcohols 4L, (methanol, ethanol, propanol, butanol). Also acetone, acetic acid, hydrochloric acid, sulfuric acid, nitric acid, acetonitrile. There is a water sprinkler system in here.

Location: Entire room.

Risk: *Fire/Explosion/Risk of adding fuel to fire*
Description: Class I & II flammables stored here, along with acids and bases.
Timing: 0-10 Minutes (First Response)
Events: Structural Damage, Fire
Mitigation: Fire team

Resources

EMS Equipment/Ambulance if personnel are injured



MSU data retention guidelines. The following information is quoted from *Research Data: Management, Control, and Access,* http://rio.msu.edu/research_data.htm.

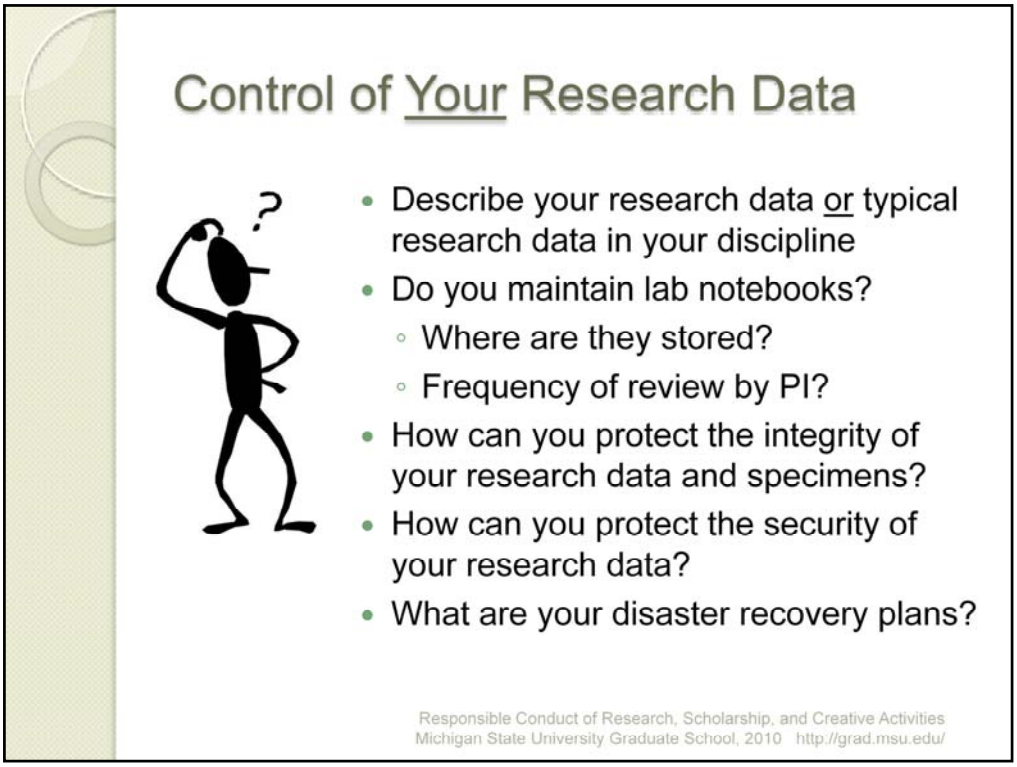
"Research data must be archived for not less than three years after the submission of the final project report or publication, whichever occurs last, with original data retained wherever possible. This should include prudent provision of off-site back up of electronic and hard-copy data. In addition, any of the following circumstances may justify longer periods of retention:

1. Data must be kept for as long as may be necessary to protect any intellectual property resulting from the work
2. If any charges regarding the research arise, such as allegations of misconduct in research or financial conflict of interest, data must be retained until such charges are fully resolved
3. If a student is involved, data must be retained at least until the degree is awarded or it is clear that the student has abandoned the work.

Beyond the period of retention specified here, the destruction of the research record is at the discretion of the PI and his or her department or laboratory. The PI should make a permanent record describing the destroyed data and the destruction date."

Other policies for data retention:

- MSU = 3 years after submission of the final project report or publication
- NIH = 3 years after date of final financial report
- FDA = 10 years for non-clinical research studies
- US Patent Office = 23 years after issue of patent for original data supporting patent claims

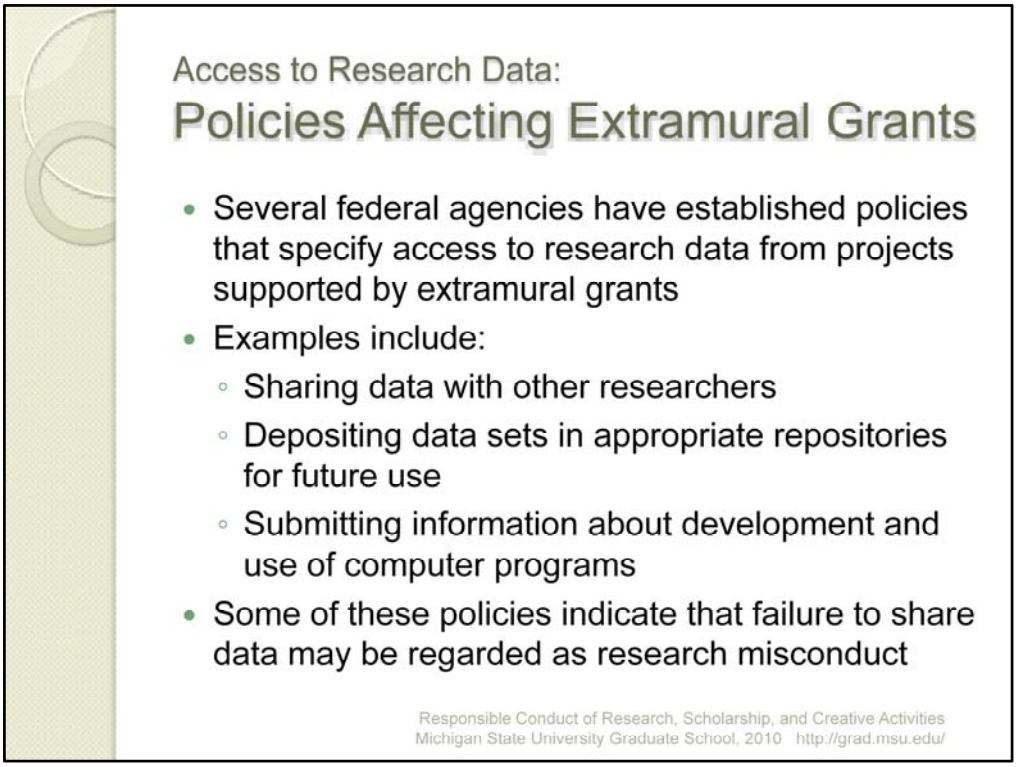


This slide calls for discussion of ways to protect research data in your discipline.

Refer to the list of data you compiled when studying Slide #6. Talk with your mentor and colleagues about best practices. If you are a mentor, educate your students/trainees about best practices.

Part 3: Access to Research Data

- Who has access?
- Conditions of access
- Security considerations



The following information about extramural grants is quoted and reformatted from *Ensuring the Integrity, Accessibility, and Stewardship of Research Data in the Digital Age* (pp. 52-53), National Academies Press, Washington, DC, 2009.

Are grantees required to share data with other researchers (privacy and national security-related exceptions are assumed)?

Yes – NIH, NSF, HHS, EPA, NASA

No – USDA, DOC, DOEd, DOE

Not stated – AFOSR, ONR

Are grantees required to deposit data sets in appropriate repositories?

Yes – NIH, NSDF, HHS, NASA

No – USDA, DOC, DOE, EPA

Not stated – AFOSR, ONR

Not applicable – DOEd

Are grantees required to submit all information regarding computer programs developed or used during the time frame of the grant?

Yes – HHS, EPA

Encouraged - NSF

No – USDA, DOC, DOEd, DOE

Not stated – NIH, AFOSR, ONR, NASA

Are printed "research misconduct" statements in effect, or a link provided to the federal policy?

Yes – NIH, NSF, USDA, DOC, AFOSR, ONR, DOEd, DOE, HHS, EPA, NASA

Researchers involved in group investigations have rights to access to data gathered by all members of the group *(Research Data: Management, Control, and Access,* http://rio.msu.edu/research_data.htm). Thus it is incumbent upon the PI to:

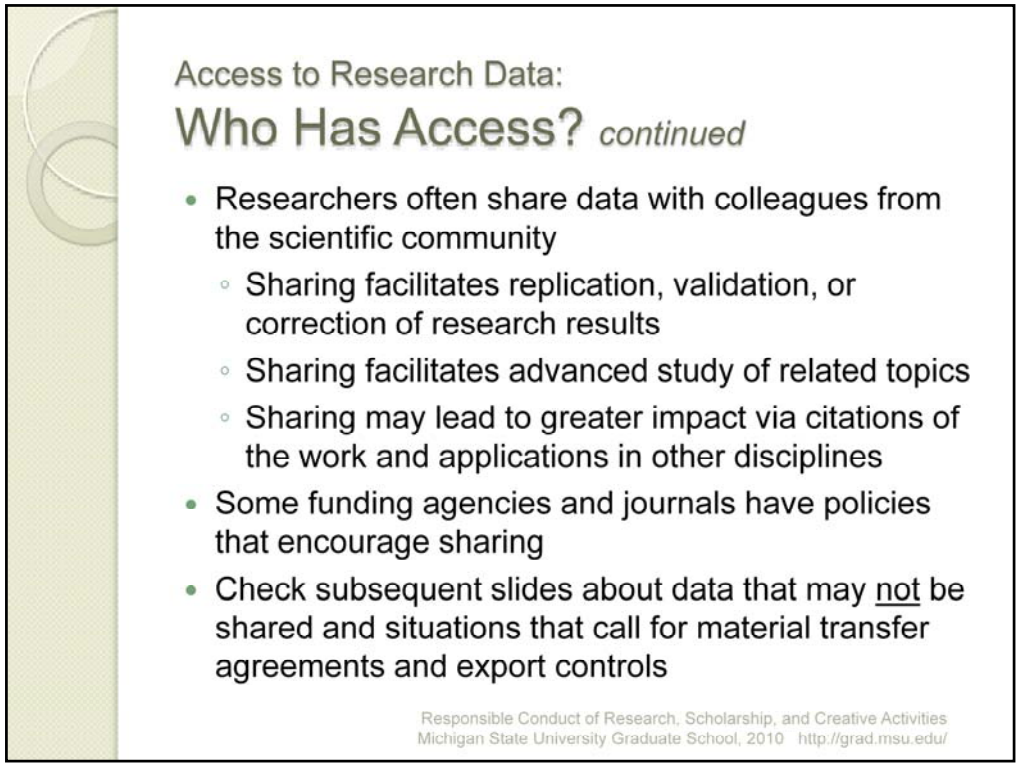
1. Design a data management scheme that insures careful data collection, data storage, and data retention provisions.
2. Educate members of the research about their responsibilities to the project, including data collection, data storage, data retention, and knowledge about responsible conduct of research.

Impact of the Patriot Act of 2001 and the Bioterrorism Act of 2002. Source: Albert H. Teich. (2004). Don't Let Science Become Another Victim of 9-11. *The Scientist, 18*(10), available at http://www.the-scientist.com/ yr2004/may/opinion_040524.html

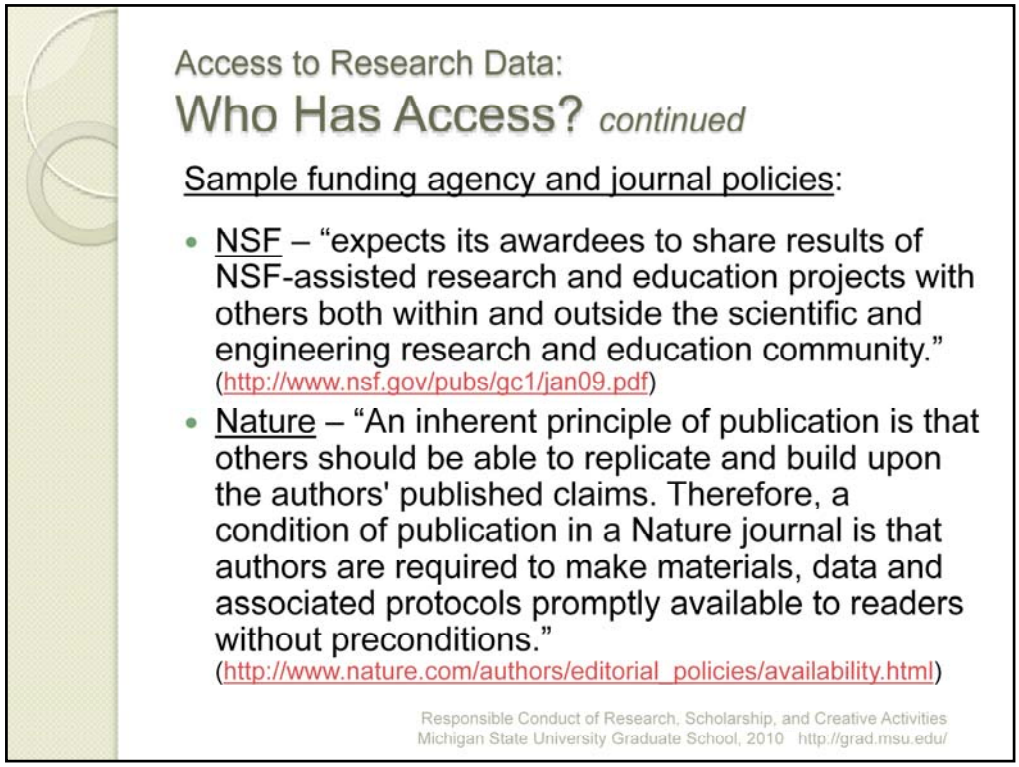
- It is more difficult for foreign students and visitors to obtain approval to come to the USA to study and work. They often experience lengthy delays and denials in visa processing.
- This situation is causing a potential "brain drain" in research. Nearly 40% of the US engineering faculty, 1/3 of US Nobel scientists, and 25% of National Academy of Science members are foreign born. Plus other scientists around the world received their PhDs or did post docs in the USA
- These rules and regulations are intended to keep sensitive materials out of dangerous hands.

Access to Research Data:
Who Has Access? *continued*

- The PI is required to provide access to research data and research records for investigations and audits, even after publication of results or after the PI leaves the university
- Investigations and audits may occur because of:
  - Alleged misconduct
  - Possible conflicts of interest or conflicts of commitment that may bias research results
  - Possible non-compliance with IRB, IACUC, and ORCBS approved protocols
  - Possible non-compliance with journal policies



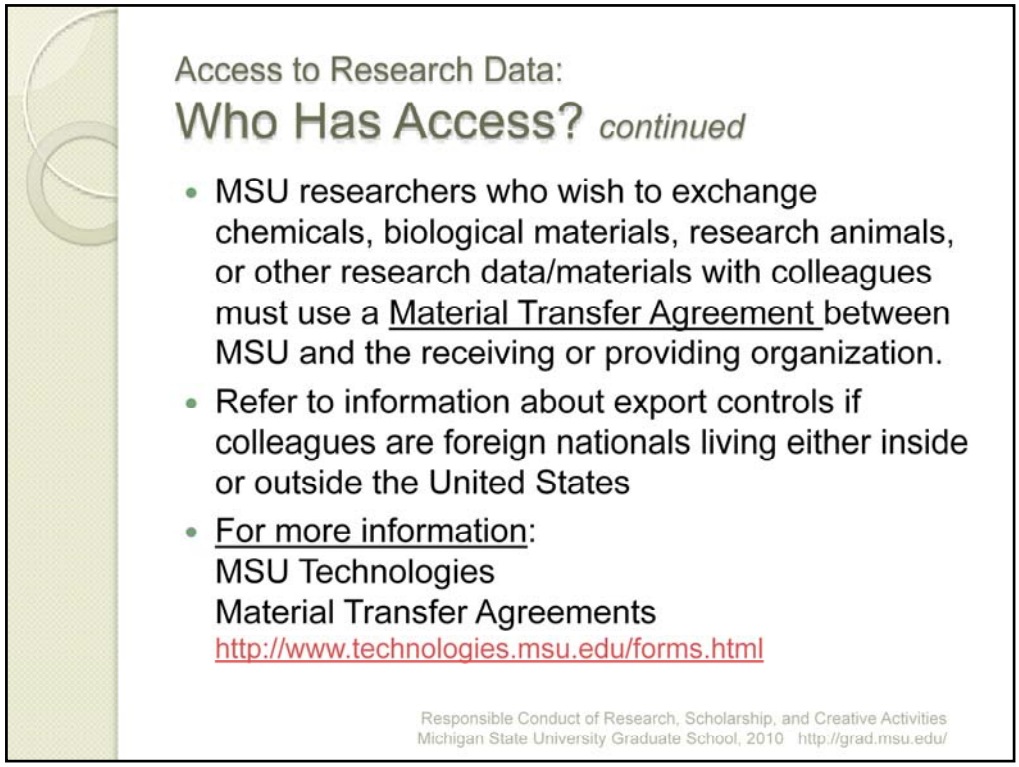
The suggestions on this slide were adapted from:
http://www.ed.ac.uk/schools-departments/information-services/services/research-support/data-library/research-data-mgmt/data-sharing/sharing-research-data



NSF refers to the National Science Foundation.

Nature is a professional journal that publishes original research.

Here is the NIH (National Institutes of Health) policy: "The NIH expects and supports the timely release and sharing of final research data from NIH-supported studies for use by other researchers." (http://grants.nih.gov/grants/guide/notice-files/NOT-OD-03-032.html)



The following text is quoted directly from *Material Transfer Agreements: Why and When?*, MSU Intellectual Property Office, (https://www.msu.edu/~vprgs/rnspr06/mta.htm)

The transfer of materials between universities and research groups at other organizations is an important aspect of scientific cooperation. Researchers may wish to exchange chemicals; plant-, human-, animal-derived material; research animals, or any number of other materials in order to facilitate a collaboration, open a new line of questioning, or help confirm research findings. Materials may be exchanged between universities, between Michigan State and another non-profit organization, or between Michigan State and a commercial entity.

When materials are being transferred it is important to ensure that

- the intellectual property rights of the receiving and the providing organization are addressed
- any special shipping needs are handled
- the university has a record of the types of materials that are entering the campus
- any attendant health and safety risks are identified and prudent provision is made to address them
- confidentiality is appropriately maintained

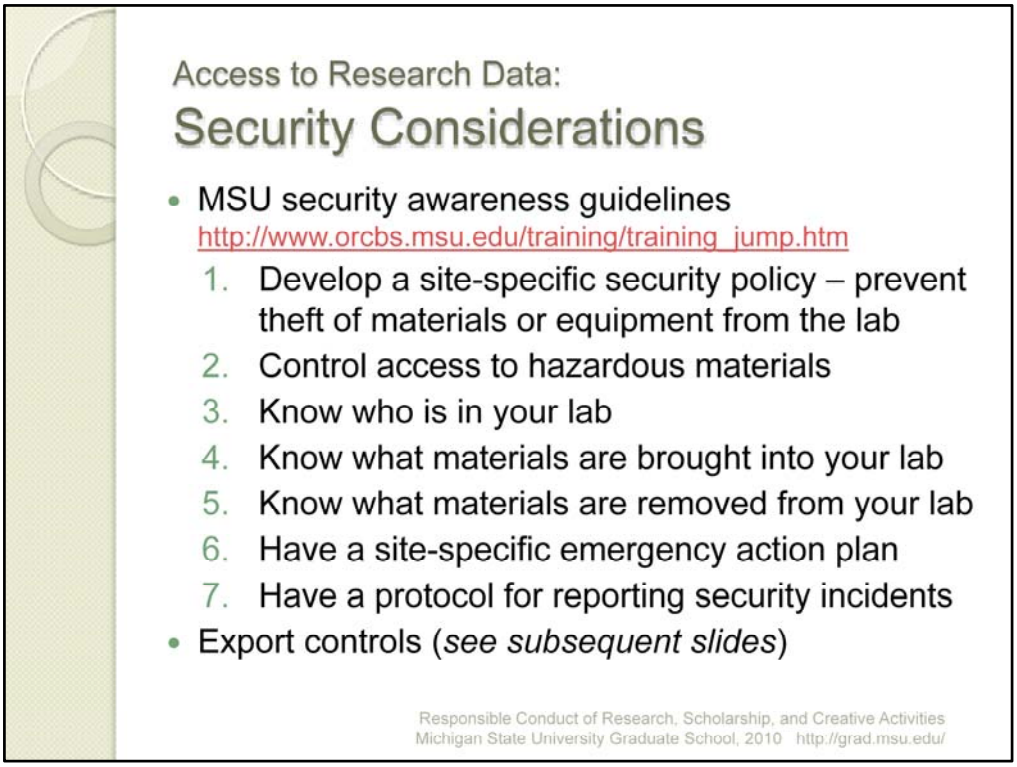
These concerns are addressed in part through the use of a material transfer agreement (MTA) between Michigan State and the receiving or providing organization.

Access to Research Data:

Conditions of Access

The PI may specify conditions for access, e.g.,

- View in lab setting only
- View photocopies only
- Pay for access/copies (especially when there are photocopy, postage, or other costs associated with sharing)
- Wait until after data are published
- Wait until patent/copyright time has elapsed
- Sign a confidentiality agreement (especially for sensitive human subjects data)



MSU security awareness guidelines (http://www.orcbs.msu.edu/training/training_jump.htm):

1. Policy - Recognize that laboratory security is related to but different from laboratory safety and develop a site-specific security policy – prevent theft of materials or equipment from the lab: (a) assess the lab for hazardous materials; (b) develop and implement lab security procedures for your lab group; and (c) train your lab group on these security procedures and assign responsibilities appropriately.
2. Control access to areas where hazardous materials are used and stored: (a) close and lock laboratory doors; (b) do not leave hazardous materials unattended or unsecured; and (c) lock freezers, refrigerators, storage cabinets, etc. where hazardous materials are stored.
3. Know who is in your laboratory area: (a) use a logbook or carded access; (b) limit access to individuals who can safely be in the lab or need to be in the lab; (c) consider the use of ID badges; (d) restrict off-hours access to individuals authorized by the PI; and (e) consider the use of guest badges and escorts where needed.
4. Know what materials are being brought into your lab: (a) know what hazardous materials are being ordered and shipped to your lab; (b) screen all packages; (c) dispose of unneeded hazardous materials promptly and properly; (d) use a log to sign highly hazardous materials in and out of secure storage; and (e) take periodic inventory of all highly hazardous chemicals, biological agents, and toxins.
5. Know what materials are being removed from your lab: (a) track the use and disposal of hazardous materials; (b) require written permission from the PI prior to removal of highly hazardous materials from the lab; and (c) promptly report any missing inventory to the Department of Police and Public Safety.
6. Have a site-specific emergency action plan (EAP): (a) recognize that controlling access can make emergency response more difficult; (b) evaluate the EAP with administrators, safety, and security officers; (c) review the EAP with lab personnel regularly; (d) provide emergency responders with information about serious hazards; and (e) include back-up and urgent access provisions for data within the EAP.
7. Have a protocol for reporting security incidents: (a) PIs should have policies for incidents such as undocumented visitors, missing hazardous materials, or unusual or threatening phone calls; and (b) train laboratory staff on procedures.

Exports include, but are not limited to:

1. Items such as software, commodities, technology, and biological agents that are either sent to a foreign destination or shared with a foreign national who is in the United States
2. Release or sharing of restricted technology or data (orally or in writing) with foreign nationals

Exports may be strategically important if:

1. The nature of the export has actual or potential military applications or economic protection issues
2. Government concerns about the destination country, organization, or individual (some countries face trade restrictions or sanctions by the United States)
3. Government concerns about the declared or suspected end use or the end user of the export

Penalties for violations of export control laws may include fines up to $1 million per violation and up to 10 years of incarceration per violation

The list of circumstances is quoted from http://research.utk.edu/exportcontrol/know.shtml

The list of circumstances is quoted from http://research.utk.edu/exportcontrol/know.shtml

"Fundamental research means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons."
National Security Division Directive, http://www.fas.org/irp/offdocs/nsdd/nsdd-189.htm.

University research does not qualify as fundamental research if:

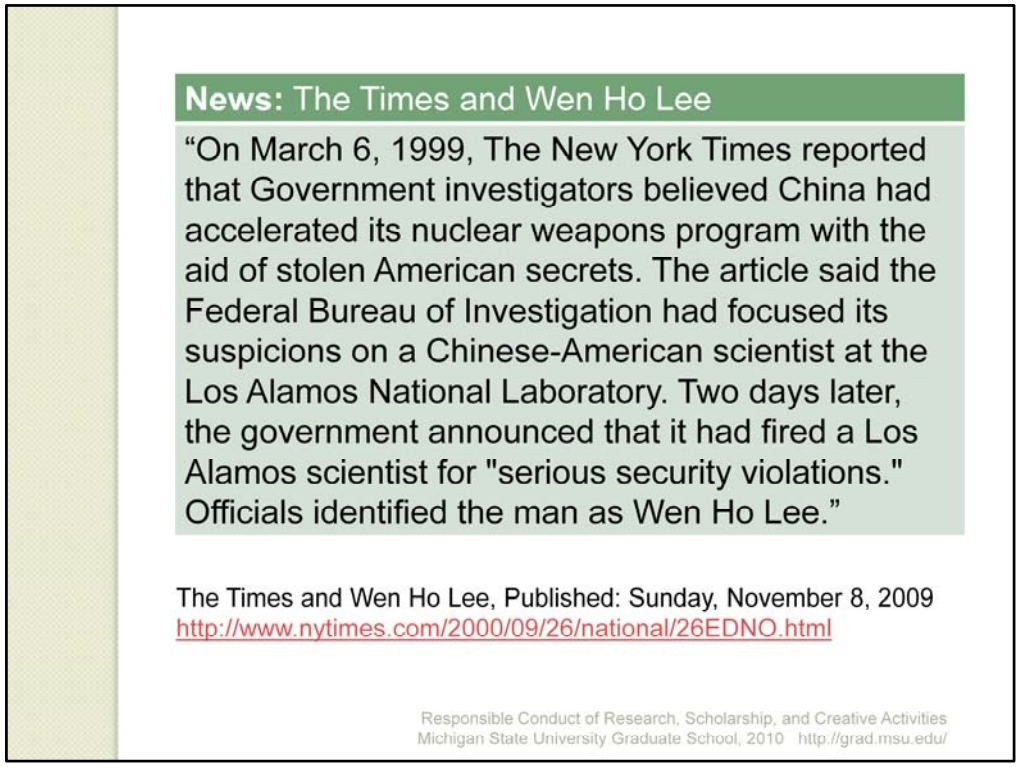
- The university accepts any restrictions on the publication of the information resulting from the research – with the exception of limited prepublication reviews by research sponsors to prevent inadvertent divulging of proprietary information provided to the researcher by the sponsor or to insure that publication will not compromise patent rights of the sponsor; or
- The research is federally funded and specific access and dissemination controls regarding the resulting information have been accepted by the university or the researcher.

Access to Research Data:

Export Controls, *continued*

For more information:

Office of Export Controls
Michigan State University
105B Olds Hall
East Lansing, MI 48823-1313
Phone: (517) 884-2300
Email: export@msu.edu
Web: http://www.exportcontrols.msu.edu/



The following information is quoted directly from The New York Times:

The Times and Wen Ho Lee, Published: Sunday, November 8, 2009,
http://www.nytimes.com/2000/09/26/national/26EDNO.html

On March 6, 1999, The New York Times reported that Government investigators believed China had accelerated its nuclear weapons program with the aid of stolen American secrets. The article said the Federal Bureau of Investigation had focused its suspicions on a Chinese-American scientist at the Los Alamos National Laboratory. Two days later, the government announced that it had fired a Los Alamos scientist for "serious security violations." Officials identified the man as Wen Ho Lee.

Dr. Lee was indicted nine months later on charges that he had transferred huge amounts of restricted information to an easily accessible computer. Justice Department prosecutors persuaded a judge to hold him in solitary confinement without bail, saying his release would pose a grave threat to the nuclear balance.

This month the Justice Department settled for a guilty plea to a single count of mishandling secret information. The judge accused prosecutors of having misled him on the national security threat and having provided inaccurate testimony. Dr. Lee was released on the condition that he cooperate with the authorities to explain why he downloaded the weapons data and what he did with it.

This slide calls for discussion of ways to manage control to your research data.

Refer to the list of data you compiled when studying Slide #6. Talk with your mentor and colleagues about best practices. If you are a mentor, educate your students/trainees about best practices.


Part 4: Ownership of Research Data
Who owns research data
Transfers of research data
Responsible Conduct of Research, Scholarship, and Creative Activities
Michigan State University Graduate School, 2010 http://grad.msu.edu/

The following passage is reproduced from *Research Data, Management, Control, and Access* (http://rio.msu.edu/research_data.htm)

Ownership: The University's claim to ownership and stewardship of the scientific records for projects conducted at the University, under the auspices of the University, or with University resources is based on both regulation (OMB Circular A-110, Sec. 53; 42CFR, Part 50, Subpart A) and sound management principles.

Michigan State University's responsibilities include, but are not limited to:

1. Complying with terms of sponsored project agreements
2. Ensuring the appropriate use of animals, human subjects, recombinant DNA, etiological agents, radioactive materials, and the like
3. Protecting the rights of faculty, students, postdoctoral scholars, and staff, including, but not limited to, their rights to access data from research in which they participated
4. Securing intellectual property rights
5. Facilitating the investigation of charges, such as misconduct in research or financial conflict of interest
6. Responding to legal actions involving the University related to research carried out under its auspices.

In grant proposals to federal agencies, some of these responsibilities are guaranteed via federal assurances agreements.

Ownership of Research Data:

Transfer of Research Data

- The PI must retain original data and research records at MSU
- When researchers (including students) leave MSU, they may take copies of research data for projects on which they have worked
- If the PI leaves and a project is moved to another institution, ownership or custody of the original data may be transferred with approval of the Vice President for Research and Graduate Studies and written agreement from the PI's new institution

Part 5: Disputes

- Disputes about data management

Disputes about Data Management

- Seek information and advice from the MSU Research Integrity Officer (RIO)
  - Jim Pivarnik, Ph.D.
    107 Olds Hall
    (517) 432-6698
    rio@msu.edu
  - Web site URL - http://www.rio.msu.edu/
- Conversations with the RIO are confidential
- Having a conversation with the RIO does not mean you are initiating a complaint – only that you are seeking information and advice

Sources

- *Research Data: Management, Control, and Access*, http://rio.msu.edu/research_data.htm
- *Ensuring the Integrity, Accessibility and Stewardship of Research Data in the Digital Age*, National Academies Press, Washington, DC, 2009. Read online at http://www.nap.edu/catalog.php?record_id=12615#description
- *On Being a Scientist: A Guide to Responsible Conduct in Research*, 3rd edition, 2009 http://books.nap.edu/openbook.php?record_id=12192&page=R1

Sources, *continued*

- *Secure Computing*, computing.msu.edu
  http://computing.msu.edu/facultystaff/documents/SecureComputing.php
- MSU Technologies
  http://www.technologies.msu.edu/forms.html
- MSU Office of Export Controls
  http://www.exportcontrols.msu.edu