

---

# University of Arizona Program in Research Integrity Education Monthly Newsletter

## *A Federally Mandated Compliance Education Program*

---

April 1, 2007

Volume 7, No. 4

This is the last newsletter in a series of Program in Research Integrity Education (P.R.I.E.) newsletters which has focused on the nine core topics in the Responsible Conduct of Research (RCR). This month the newsletter is highlighting the topic of “*Research Misconduct*.”

The information presented below is authored by Michael Kalichman and P.D. Magnus and may be viewed at the *RCR Education Resources* web site, which is: <http://rcrec.org/r/index.php>.

---

### **Responsible Conduct of Research (RCR)**

---

P.D. Magnus and Michael Kalichman,  
September 2002

### **Research Misconduct**

---

#### **Background**

There are some indications that research misconduct occurs only rarely. In 20 years, the federal government found an average of about 10 cases of research misconduct per year; that is, about one case per year for every 10,000 researchers. However, there are many barriers to accurately quantifying the extent of research misconduct; cases may go unreported and institutions may be biased against finding misconduct. The actual rate of research misconduct could be as low as 1 in 100,000 or as high as 1 in 100. (Steneck, 2000)

In the past 20 years, numerous serious cases of alleged misconduct have been widely publicized. In many cases, the allegations were borne out by subsequent investigation. It is noteworthy that in these cases both whistleblowers and those accused of wrongdoing paid a price whether the allegations were ultimately sustained or not.

#### **Rules and regulations**

Some, but not all, categories of questionable conduct are covered under the current Public Health Service (PHS) policies in the Code of Federal Regulations (PHS, 2000a). Under these regulations, research misconduct is defined as: fabrication, falsification, plagiarism, or other practices that seriously deviate from those that are commonly accepted within the scientific community for proposing, conducting, or reporting research.

Minimally, for something to count as research misconduct it must be committed intentionally, knowingly, or recklessly, and there must be a significant departure from accepted practices of the relevant research community.

Although not yet finalized, a new government-wide definition of research misconduct was recently approved by the Office of Science and Technology Policy (OSTP, 2000), and in 1999 the Secretary of the Department of Health and Human Services announced plans to adopt a similar definition through rulemaking (DHHS, 1999). The most significant proposed changes would restrict the definition of research misconduct to fabrication, falsification, and plagiarism. In the OSTP proposal, “research misconduct” is defined as: fabrication, falsification, or plagiarism in proposing, performing, or reviewing research, or in reporting research results.

For research funded by the Public Health Service (PHS), the procedures for responding to allegations of research misconduct are currently covered in the Code of Federal Regulations (PHS, 2000b). It has been proposed that this regulation be replaced by a single federal policy announced in December of 2000 (OSTP, 2000). The existing and proposed definitions both make it clear that federal agencies and research institutions have a shared responsibility for the research process and, therefore, for responding to allegations of research misconduct. There are a range of circumstances under which institutions must report allegations to federal authorities (see italicized section below); in other circumstances, allegations of research misconduct are initially in the purview of individual institutions.

To foster fair and timely responses to allegations of research misconduct, both current and proposed regulations include safeguards for informants and for the subjects of allegations, an expectation of objectivity and expertise, adherence to reasonable time limits, and respect for confidentiality.

*Research institutions are required to notify the appropriate federal agency if an allegation of research misconduct involves federally funded research; if the institution's inquiry finds that an investigation is warranted; if there is an immediate health hazard involved; if there is an immedi-*

*ate need to protect federal funds or equipment; if there is an immediate need to protect the interests of the whistleblower or of the subject of the allegations; if it is probable that the alleged incident is going to be reported publicly; if there is a reasonable indication of possible criminal violation. (42CFR50.104(b); PHS, 2000b)*

## **Principles**

### **The integrity of science depends on the integrity of research.**

Science is predicated on trust – without confidence in the integrity of their peers, scientists would be unable to trust one another's work. The demands of ethical and responsible conduct may not always seem expedient.

### **The integrity of research depends in part on self-policing.**

Just as peer review operates to assure the legitimacy of published reports, self-policing operates to assure the legitimacy of research at a deeper level. This means that scientists should be familiar with definitions of research misconduct and procedures for dealing with it, regardless of whether they are actually party to allegations. Self-policing also demands that scientists attempt to communicate with one another to foster an environment in which responsible research is explicitly discussed and encouraged.

## **Guidelines**

### **Documentation**

A failure to keep good records can have serious consequences for the progress of a research project, but can be particularly devastating for someone involved in an allegation of misconduct. Whether one is making the allegation or accused of misconduct, clear documentation of who did what, and when they did it will provide the best chance for a fair and timely resolution.

As with good research, an allegation of misconduct should be sustained or rejected based on adequate documentation. An allegation of research misconduct is one of the most serious charges that can be made against a scientist. As such, it is essential that a charge be sustained only if justified by documentation and other relevant evidence. Correspondingly, it would be unusual to have an allegation of misconduct based solely on a disputed testimonial account.

### **Rules and procedures**

Although institutions receiving federal funds need to meet a common set of minimal requirements, individual institutions are granted substantial leeway in the rules and procedures for handling of allegations of misconduct. Especially if you become involved in an allegation of

misconduct, it is in your best interest to familiarize yourself with all relevant institutional procedures. It is important to determine who is to be apprised of the allegation, what constitutes evidence for or against the allegation, how the evidence is to be obtained, who will review the allegation, what her or his role will in the process, and what will be the time course for reviewing the allegation.

### **Institutional channels are preferable to public channels.**

The pace of the process for dealing with alleged misconduct may be frustrating. In such circumstances, it can be tempting to discuss the case publicly. Placing a complex, unresolved issue into the public arena can produce unpredictable results, however, which can be harmful to the people involved and to the scientific community as a whole. Publicity may compromise the integrity of an ongoing inquiry and the privacy of parties to the investigation. Moreover, an attempt to circumvent the institutional process may prejudice those charged with reviewing the allegation.

## **Resources**

### **Works cited**

- Department of Health and Human Services (2000): Public Health Service Standards for the Protection of Research Misconduct Whistleblowers. Notice of proposed rulemaking. Federal Register November 28, 2000 65(229): 70830-70841
- Office of Science and Technology Policy (2000): Federal Policy on Research Misconduct: Notification of Final Policy. Federal Register December 6, 2000 65(235): 76260-76264.
- Public Health Service (2000a): Sec. 50.102 Definitions. Subpart A. Responsibility of PHS Awardee and Applicant Institutions for Dealing With and Reporting Possible Misconduct in Science. Part 50 – Policies of General Applicability. Chapter I – Public Health Service, Department of Health and Human Services. Title 42 – Public Health. 42CFR50.104, p. 168.
- Public Health Service (2000b): Section 50.104 Reporting to the OSI. Subpart A. Responsibility of PHS Awardee and Applicant Institutions for Dealing With and Reporting Possible Misconduct in Science. Part 50 – Policies of General Applicability. Chapter I – Public Health Service, Department of Health and Human Services. Title 42 – Public Health. 42CFR50.104, pp. 170-171.
- Steneck N (2000): Assessing the integrity of publicly funded research: A background report for the November 2000 ORI Research Conference on Research Integrity.  
<http://ori.dhhs.gov/multimedia/acrobat/backgint.pdf>

## Further resources

- Brown S, Kalichman MW (1998): Effects of training in the responsible conduct of research: A survey of graduate students in experimental science. *Science and Engineering Ethics* 4: 487-498. *This study found that 50% of graduate students responding to a survey at the University of California, San Diego reported having spent a total of an hour or less discussing responsible conduct of research with their major professor or thesis advisor.*
- Department of Health and Human Services (1999): HHS Announces Plans to Improve Research Integrity and Prevent Research Misconduct. Press Release, Oct. 22, 1999 <http://www.hhs.gov/news/press/1999pres/991022.html>
- Friedman PJ (1996): Advice to individuals involved in misconduct accusations. *Academic Medicine* 71: 716-723.  
National Academy of Sciences, National Academy of Engineering, Institute of Medicine (1995): *On Being a Scientist: Responsible Conduct in Research*. National Academy Press. <http://www.nap.edu/readingroom/books/obas>

---

**UNIVERSITY OF ARIZONA  
RESEARCH SUPPORT SERVICES GROUP  
(RSSG)**

---

**HUMAN SUBJECTS  
PROTECTION PROGRAM**

**≡Highlights≡**

### **Classification of Medical Devices\***

This is the third article in a series of articles regarding classification of medical devices. As a reminder, the regulations about medical devices are found in the Code of Federal Regulations Title 21, part 800-1050. The device regulations are similar in many ways to the drug regulations, however there are several distinctions. One difference is the definition of a medical device. A medical device is distinguished from a drug in that it cannot react chemically with the body and that it is being promoted or studied for a medical purpose.

With the Medical Device Amendment of 1976, the Food and Drug Administration (FDA) established three classifications for devices. This article will focus on class III devices. Class III devices have insufficient information to determine that they are safe and effective (i.e., any new devices about which there are few or no data are automatically classified as class III). This means

that these types of devices need additional regulation in order to ensure safety and effectiveness. Examples of class III devices include implantable orthopedic prostheses (ligament, tendon, hip, knee, finger), eye valve implants (glaucoma implant), and embryoscopes and devices intended for fetal surgery.

Devices that were available on the market prior to the Medical Devices Amendment of 1976 were allowed to remain on the market without demonstrating safety for efficacy with the caveat that, at any time the FDA could ask for a submission of clinical data. Several cases of this type have occurred causing the manufacturer to conduct studies and gather information on their product that is already being marketed.

Before a class III (significant risk) device can undergo clinical investigation, an investigational device exemption (IDE) must be obtained from the (FDA). The application is normally submitted by the sponsor; however Principal Investigators who function in the role of investigator/sponsor may submit the application for review by the FDA. The decision to submit an application to the FDA carries with it a substantial regulatory impact on the sponsor. If the IDE is claimed, a letter from the Center for Devices and Radiologic Health (CDRH) should be obtained referencing the device and the indications and submitted to the Institutional Review Board (IRB) before IRB approval can be granted.

It is important to understand the level of classification particularly as it relates to class III devices. These types of devices are highly regulated and require extensive oversight in order to carefully monitor the safety and efficacy of the device.

\*Heath, E. J. (2002). Research Involving a Medical Device. In R. J. Amdur and E. A. Bankert (Eds.), *Institutional Review Board Management and Function* (pp. 434-440). Sudbury, MA: Jones and Bartlett.



### **Good Laboratory Practices: (GLP)**

The Federal Food, Drug, and Cosmetic Act and Public Health Service Act require that sponsors of FDA-regulated products submit evidence of their product's safety in research and/or marketing applications. These products include food and color additives, animal drugs, human drugs and biological products, human medical devices, diagnostic products, and electronic products. FDA uses the data to answer questions regarding:

- The toxicity profile of the test article. The observed no adverse effect dose level in the test system.
- The risks associated with clinical studies involving humans or animals.
- The potential teratogenic, carcinogenic, or other adverse effects of the test article.
- The level of use that can be approved.

The following resources are provided to help investigators, sponsors, and contract research organizations who conduct nonclinical studies on investigational new drugs to comply with U.S. law and regulations covering good laboratory practice (GLP).

- [Bioresearch Monitoring: Good Laboratory Practice](#)
- [Regulatory Pharmacology and Toxicology](#)
- [Toxicological Principles for the Safety of Food Ingredients \(Redbook 2000\)](#)
- Code of Federal Regulations: [Good Laboratory Practice for Nonclinical Laboratory Studies \(21 CFR Part 58\)](#)

Marilyn M. Marshall, SpM  
Quality Assurance Officer  
Office of the Vice President for Research  
621-1469 (p), 621-1429 (f)



## **Radiation Control**



### *MISSION: Strategic Vision of the Radiation Control Office*

The Radiation Control Office (RCO) is a mandated department responsible for maintaining the radiation health and safety of the University community and for ensuring the University's compliance with all relevant ionizing and non-ionizing radiation regulations. Radiation use occurs during research, instructional, and clinical activities on the University of Arizona campus, University Medical Center (UMC), University Physicians Health (UPH) and Southwest PET (SWP) Clinics, but may also take place at other affiliated sites through-out the state and occasionally in other states.



### **News from HIPAA.....**

#### **Two Maryland Hospitals Report Patient Privacy Security Breaches**

Reprinted from the March 2007 issue of [REPORT ON PATIENT PRIVACY](#), the industry's most practical source of news on HIPAA patient privacy provisions.

Two Maryland hospitals reported breaches of patient data within a week of each other in Febru-

ary. In both incidents, data for thousands of patients were involved, and in both cases, those data were not encrypted. One industry expert says any covered entity (CE) that is not encrypting data stored on devices "is doing so at its own peril."

The incidents involve missing backup data tapes at one facility and a stolen laptop at another hospital.

"All CEs (and all organizations working with confidential or proprietary data) should encrypt all data stored on portable devices (e.g., PDAs, laptops, smart phones, etc.) and portable media (e.g., CD ROM, flash drives, jump drives, etc.) before it leaves a facility," says Chris Apgar, president of Apgar & Associates LLC in Portland, OR. He adds that if laptops are used in public spaces, the data on the hard drive should be encrypted and locking laptop docks should be used when the device is not in use but needs to be available. "This is just plain sound security practice," he says.

"What CEs can learn from this is they are at high risk from a regulatory, legal/civil, business and reputation perspective if they do not employ encryption on portable devices and media," Apgar tells *RPP*. "They can be found in violation of the security rule, can find themselves sued, in violation of state consumer protection laws, receive a lot of bad press, lose critical data and lose the trust of their customers," he explains.

Apgar says current laws "come very close to mandating" encryption. "The HIPAA security rule, as an example, lists encryption as an addressable implementation specification," he says. "This doesn't mean optional. It means that a CE needs to implement encryption as described in the rule, implement a similar solution that provides equal protections or very thoroughly document why the implementation specification will not be followed (and cost cannot be the primary reason the implementation specification is not adopted or followed)," he explains.

In the first data breach, the Johns Hopkins Hospital in Baltimore reported on Feb. 7 that nine data tapes containing information on employees and patients were missing. The tapes had been sent to a contractor that makes microfiche backups of the data in late December, but were never returned to the hospital. Johns Hopkins realized the tapes were missing on Jan. 18, the facility explains on its Web site.

An investigation by the hospital indicates that "it is highly likely that the tapes were mistakenly left by a courier company hired by the contractor at another stop. They were thought to be trash, [were] collected and later incinerated," the Johns Hopkins Web site says.

## Many Employees, Patients Could Be Affected

Eight of the tapes contained personal information on 52,000 Johns Hopkins University employees, the hospital says. Another tape contains “less sensitive personal information” on about 83,000 patients who were either new patients seen between July 4, 2006, and Dec. 18, 2006, or who changed their demographic information during that period, according to the hospital. The information includes birth date, sex, race, mother's maiden name, father's name and medical record number. It did not include Social Security numbers, addresses or financial information.

The tapes are not compatible with a typical personal computer, Johns Hopkins says. “In order to access the data, an unauthorized person would have needed specialized equipment that most computer users do not have. The information was not encrypted, however, and was in a format that could have been read by a user who had the proper equipment,” the hospital explains. “It has not in the past been the industry standard to transport information in an encrypted form, in part because of the incompatibility of formats and equipment between vendors and customers. Johns Hopkins is changing its processes to ensure that data sent to third parties is encrypted, but that process is not yet universal,” Johns Hopkins says.

A spokesperson for the facility adds that it is “evaluating a variety of options with respect to management and handling of data, including changes in its processes.” Statements by Johns Hopkins say it is also re-evaluating its relationship with the contractor and has suspended shipments in the meantime. It is also “evaluating its processes and procedures for the handling of data,” and contacting those affected.

At St. Mary's Hospital in Leonardtown, MD, a laptop was stolen from the facility's emergency care center, the hospital announced on Feb. 14. Information on the computer includes names, Social Security numbers, and birth dates on about 130,000 patients, but the computer did not contain any patient health or financial data, St. Mary's says in a statement on its Web site.

Besides notifying all the patients involved, the hospital has contracted with National ID Recovery, a Georgia-based organization that manages situations in which data have been compromised.

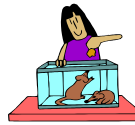
A spokesperson for St. Mary's did not return repeated calls for additional information about the incident. *The Baltimore Sun* reported that the files that are on the laptop were not encrypted. The

computer was used for registering patients as they came to the department for treatment.

Visit [www.jhu.edu/identityalert/releases/faq.html](http://www.jhu.edu/identityalert/releases/faq.html) and [www.smhwecare.com](http://www.smhwecare.com) for more information on the breaches.

Jeniece Poole, Privacy Officer  
Office of the Vice President for Research  
[jpoole@email.arizona.edu](mailto:jpoole@email.arizona.edu)

## University of Arizona – Animal Care



### Quality Care for Research Animals

## eSirius Implementation Update

University Animal Care is currently working through a second test of the conversion and migration procedure used to move data between Sirius, our current animal facility software and eSirius. This phase allows UAC and our software provider, NTM, to identify any problems occurring during conversion/migration.

Conversion testing also allows for refinement of the process so that the final migration prior to going live takes the least amount of time possible and is the most accurate.

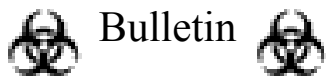
After completion of the current migration process, UAC will begin implementation and beta testing of the next version of eSirius. Version 10A offers several exciting upgrades to our current version and is the version that we will use to perform ‘live testing.’ ‘Live testing’ utilizes protocol, procurement and cage card data from Sirius that has been loaded into eSirius during the conversion and migration phase. This allows our volunteers to work with real data in a test system with no fear of impacting operational or working data.

At this point, we anticipate live testing the eSirius Protocol and Procurement processes with volunteer PIs starting in May.

After completion of ‘live testing,’ UAC and the Institutional Animal Care and Use Committee Office will begin the final ‘go live’ phase this summer, which includes fleshing out several hundred protocols in eSirius with data from existing active paper protocol records.

Please contact Andi Mitchell in the eSirius office at 626-8332 or [mitchela@u.arizona.edu](mailto:mitchela@u.arizona.edu) if you have any questions about the eSirius implementation, would like to see a demonstration of the software, or would like to volunteer to participate in eSirius ‘live testing.’

## Institutional Biosafety Committee



### Bulletin

#### Frequently Asked Questions....

**Question:** What is a Memorandum of Understanding and Agreement Form?

**Answer:** A Memorandum of Understanding and Agreement (MUA) Form is necessary to provide compliance with granting agencies and University biosafety policies. This form is available on the IBC website and at <http://mua.abc.arizona.edu/> and **should be submitted online**. After filling out the initial profile information, each subsequent submission uses this information. A separate archive will be created for all MUA forms, and can be retrieved by the user for modification and resubmittal.

If you are only going to have Biosafety Level One (**BSL-1**) research projects, a three year laboratory registration is available at the web address below. This allows the Principal Investigator to conduct low biohazard research without submitting separate MUA's for each proposal. <http://mua.abc.arizona.edu/registration/>.

---

### OPPORTUNITIES FOR ON-LINE ETHICS TRAINING

---

#### Online Research Ethics Course

This course was developed through the Practical Ethics Center at the University of Montana with Office of Research Integrity support during the 2002-03 academic year. Six course sections include: *Session One* (Ethical Issues in Research); *Session Two* (Interpersonal Responsibility); *Session Three* (Institutional Responsibility); *Session Four* (Professional Responsibility); *Session Five* (Animals in Research); *Session Six* (Human Participation in Research).

The following web address contains more information regarding this valuable online course: [http://ori.hhs.gov/education/products/montana\\_round1/research\\_ethics.html](http://ori.hhs.gov/education/products/montana_round1/research_ethics.html)

#### Ethical Guidelines for Gifts to Physicians from Industry

*Free educational modules now available*

The American Medical Association's (AMA) national initiative on *The Communication of Ethical Guidelines for Gifts to Physicians from Industry* is now offering four free online modules for CME credit. Each educational module is available in two formats:

- Online self-study for CME credit; and
- Downloadable resources educators can use to build one-hour learning experiences.

These educational modules will help satisfy Accreditation Council for Graduate Medical Education (ACGME) requirements for education on professionalism and industry professional relationships, as well as similar requirements by the American Board of Medical Specialties (ABMS).

For more information, you may visit the following internet web address: <http://www.ama-assn.org/ama/pub/category/8405.html>.

#### On-Line Module or Short Course in "The Ethics of Research with Human Subjects" *The Least of My Brothers*

Funded by the [National Institutes of Health](#)  
(Grant Number 1 T15 AI07601)

*The Least of My Brothers* is an on-line module (or short course) in the ethics of research with human subjects. For more details and course information, please access the following internet web address: <http://poynter.indiana.edu/sas/lb/>, or you may also contact Kara Lochridge at: (812) 856-4968, or [klochrid@indiana.edu](mailto:klochrid@indiana.edu).

---

### Upcoming Conferences/Workshops

---

**May 15-18, 2007**

14<sup>th</sup> Annual Teaching Research Ethics Workshop  
Indiana Memorial Union, Bloomington, IN  
[Register](#) now for the Fourteenth Annual  
[Teaching Research Ethics Workshop](#).

**May 31 – June 1, 2007**

*Costs and Benefits of Responsible Conduct of Research  
Education Programs*  
Minneapolis, MN  
Co-sponsor: University of Minnesota

**September 17-19, 2007**

*First World Conference on Research Integrity*  
Lisbon, Portugal  
Co-sponsor: European Science Foundation  
To pre-register: [www.esf.org/conferences/researchintegrity](http://www.esf.org/conferences/researchintegrity)

---

#### University of Arizona Program in Research Integrity Education staff:

Alice C. Langen, Director, Research Compliance  
Ruth K. Daniels, Program Coordinator and Editor of the  
P.R.I.E. Newsletter [rhk@u.arizona.edu](mailto:rhk@u.arizona.edu)  
P.R.I.E. – Program phone number: (520) 626-6282  
*The P.R.I.E. newsletter is researched  
and compiled by Ruth Kurash Daniels.*

---

#### Words of Wisdom:

*"It still holds true that man is most uniquely human when he turns obstacles into opportunities."*

— Eric Hoffer