



June 15, 2020

Via Email to OASH-ORI-Public-Comments@hhs.gov

Elisabeth A. Handley
Director, Office of Research Integrity
1101 Wootton Parkway, Suite 240
Rockville, MD 20852

RE: Sequestration RFI

Dear Director Handley:

The Council on Governmental Relations (COGR) is an association of 187 public and private U.S. research universities and affiliated academic medical centers and research institutes. COGR concerns itself with the impact of federal regulations, policies, and practices on the performance of research conducted at its member institutions. One area of significant interest and expertise among COGR member institutions is ensuring the integrity of basic, animal and human subjects research.

COGR appreciates the opportunity afforded by the Office of Research Integrity (ORI) to provide information in response to the April 29, 2020, Request for Information (RFI) [[85 FR 23834](#)] concerning the sequestration of digital data, as required under the regulations governing processes for the inquiry and/or investigation into allegations of research misconduct in Public Health Service (PHS) funded research. [[42 CFR §93.305\(a\)](#)]. The questions raised in the RFI are addressed below.

What unique challenges exist when collecting digital data and what approaches successfully address them?

The ease of copying, modifying, deleting, and transmitting digital data, along with the fact that digital data can be stored on multiple different types of devices and systems make it difficult to ensure that institutions have taken custody of “all of the research records and evidence needed to conduct the research misconduct proceeding.” [[42 CFR §93.305\(a\)](#)]. These characteristics inherent to digital data make it difficult for institutions to (a) determine the universe of data to be collected; and (b) identify and gain access to the sources (e.g., devices, systems) on which the data is stored. Each of these challenges is addressed below in answer to the specific RFI questions on these topics.

An additional challenge unique to digital data is technological inaccessibility because software used to interpret or access the data is no longer available, or because the data is kept on a device that is broken or no longer accessible because it has become obsolete (e.g., antiquated lab instruments, floppy disks, etc.)

Finally, unlike hardcopy records, which can easily be obtained and photocopied, best practices for

sequestration require the imaging of devices and electronically copying data. Many cloud-based data storage systems, however, cannot be imaged, and may alert the user (respondent) when accessed. Given the wide disbursement of electronic data across many different devices/systems, as well as the need for digital search strategies to sort through captured data, sequestration in research misconduct cases frequently requires technological expertise. This is particularly true in cases that involve a large amount and/or variety of digital data and in cases involving multiple research projects or multiple labs, where maintenance of metadata to assess digital data creation and access is critical. Certain digital data storage and sharing methods that permit multiple users to edit a document (e.g., Dropbox, Google Docs) may introduce additional challenges in that some platforms may not retain metadata that may be relevant in the review of a misconduct matter.

Institutions frequently need to supplement in-house information technology (IT) personnel with costly consultants, as well as incur costs for hardware, software and storage mechanisms used to sequester and/or access, track and/or use the data that has been sequestered. Unfortunately, even these time-consuming and costly additions may prove ineffective, as consultants are generally more experienced with capturing information for civil litigation, and thus frequently fail to account properly for the unique institutional environment or the specific and unusual needs of the research misconduct review process.

Institutions have adopted both administrative and technical approaches to dealing with problems inherent in sequestering digital data. Administrative solutions include institutional, school or unit policies that require research data to be maintained in an organized fashion, kept on certain systems or devices, and backed up on a regular basis (*see, e.g., [New York University, Policy on Retention of and Access to Research Data](#); [University of Iowa, Institutional Data Policy](#)*), and policies that require personnel to provide access to digital data in connection with investigations (*see, e.g., [Stanford University, Retention of and Access to Research Data](#), Sec. 6; [Northwestern University, Research Data: Ownership, Retention, and Access](#), Sec. 1.0*). Technical solutions include the purchase and use of electronic laboratory notebooks or similar systems for storing data. [*See, e.g., [MIT Libraries, Data Management](#) (enterprise license to LabArchives electronic lab notebook); [University of Wisconsin-Madison Information Technology, Electronic Lab Notebooks](#) (provision of LabArchives digital notebook service)*]. Along with these technical tools, a number of institutional libraries (or other central research units) offer researchers assistance in developing and implementing data management plans. [*See, e.g., [Duke University Libraries, Research Data Management](#); [The Ohio State University Libraries, Research Data Management – Best Practices](#)*]. The feasibility of implementing each of these types of support and tools would be enhanced by increasing the portion of grant funding allocated to data management, retention, and storage, particularly long-term retention of primary data necessary to evaluate allegations when they arise.

How do institutions identify sources of digital data that need to be sequestered?

The identification of data relevant to the inquiry/investigation is the first, and often most difficult, step in a successful sequestration effort. When research misconduct allegations come from a member of the team that conducted the research, that individual can provide guidance in identifying the sources of data that should be sequestered. Additionally, institutional and lab information technology (IT) personnel provide Research Integrity Officers (RIOs) with information about where labs keep data on institutional servers and lab devices.

When allegations come from outside the lab (e.g., journal report of potentially falsified images), however, there may not be anyone other than the lab personnel themselves to assist the RIO in

identifying what systems, devices and computers house relevant digital data, a situation that presents obvious conflicts. The need to rely on potential respondents to identify data to be sequestered is more likely to arise in the case of digital data because of the simple fact that this data is typically password protected and/or account specific. Even when digital data can be institutionally accessed without an individual's password and/or their assistance in accessing an account, deciphering lab and individual data naming conventions without the guidance of someone familiar with the data is arduous. Finally, although institutional best practices for sequestration generally include forensic imaging and copying of lab computers and devices, it is difficult for someone with limited knowledge of the lab's practices to parse through the copied files and identify relevant data.

Identifying data to be sequestered can be particularly difficult at the beginning of an inquiry because all respondents and/or affected research may not yet be identified. Digital data is easy to delete/destroy, and persons who have committed research misconduct, but have not yet been identified as respondents, may be tempted to take this course. Although, federal regulations state that the "destruction, absence of, or respondent's failure to provide research records adequately documenting the questioned research is evidence of research misconduct" this is only the case when the institution establishes by a preponderance of evidence that:

[T]he respondent intentionally, knowingly, or recklessly had research records and destroyed them, had the opportunity to maintain the records but did not do so, or maintained the records and failed to produce them in a timely manner and that the respondent's conduct constitutes a significant departure from accepted practices of the relevant research community." [42 CFR 93.106].

In the case of digital data this standard poses a particularly difficult evidentiary hurdle given that computers routinely break and/or are lost, stolen, destroyed and hacked. In fact, many research misconduct cases involve a stolen laptop or crashed hard drive at some point during the proceedings.

Digital data may be located on devices not necessarily owned by the institution, such as personal computers and storage devices, cloud-based and online series, and personal email. What approaches are successful in securing data in these situations? What data policies address this issue?

Digital data is very portable; thus, it is not unusual for persons within a lab (or in multiple labs) to hold data on multiple institutional and personal devices and systems. Gaining access to data stored on institutional devices and systems is typically addressed through institutions' computing acceptable use policies or research data policies. Acceptable use and/or research data policies provide institutional device and network users with a description of the circumstances under which the institution may access information, including access for investigations. [See, e.g., [Brown University, Computing & Information Services, Acceptable Use Policy](#); [University of Kentucky, Data Retention and Ownership Policy](#)]. Frequently, these policies make clear that all research data (or in some case research data produced for grants and contracts) is the property of the institution and can be accessed by the institution without interference. [See, e.g., [Stanford University, Retention of and Access to Research Data](#), Sec. 4; [Yale University, Research Data & Materials Policy](#), Sec. 6001.1]. Acceptable use/research data policies generally include email systems as well, although processes for accessing email may include greater safeguards (e.g., additional levels of review). [See, e.g., [Villanova University, Email Policy, Section 2.3](#); [Harvard University, Policy on Access to Electronic](#)

[Information](#)]. The scope of these policies, however, may not always clearly address situations in which researchers leave for another institution and take with them institutional data stored on a personal device and/or import the data onto a device at the other institution.

Institutions take different approaches with respect to the use of personal devices. Some institutions may require the use of institutional-owned devices to conduct business, while others also permit the use of personal devices. In the case of students and post-docs, institutions frequently do not have the resources to supply these individuals with institutional computers, and instead rely on them to supply their own. Institutions that permit personal devices to be used for institutional purposes, including research, may have policies that require the device owner to provide the institution with access to institutional information kept on the device. [See, e.g., [University of Michigan, Security of Personally Owned Devices that Access or Maintain Sensitive Institutional Data](#); [University of Chicago, Policy on Information Technology Use and Access](#)]. Even when policies include the right to access personal devices that contain institutional information, the logistics can be complicated if the employee or student does not voluntarily agree to make the device available. The situation can be further complicated if the employee or student has left the institution, making it significantly more challenging to gain access to the personal device, particularly, if the employee or student has relocated outside of the United States. Finally, the use of legal process to obtain the device is frequently impracticable and unlikely to provide the timely access necessary in a sequestration process.

Challenges also arise when research misconduct cases span institutions, resulting in the need to coordinate cross-institution sequestration and transfer of digital data. For example, data supporting the research may be kept at another institution because a laboratory moved from one institution to another or the research may involve a multi-institution collaboration. Institutions in the United States that are subject to the PHS regulations frequently cooperate with their peer institutions. When the sequestration request involves research over which an institution does not have jurisdiction (i.e., research conducted by a faculty member before he/she came to work at the institution), it may be reluctant to become involved. Similarly, institutions that are not subject to the PHS regulations and/or not located in the U.S. may be hesitant to assist in sequestering data on their systems/devices.

What is the technical makeup of successful teams [that institutions assemble to assist in gathering and securing evidence], especially regarding digital evidence? How are members of these teams selected and trained?

Many larger institutions have IT personnel who are assigned to assist in the sequestration of digital data. These personnel often have computer security backgrounds and experience in forensically imaging devices. Institutions with more limited resources and/or less experience in handling research misconduct cases may not have these IT resources available and may not be able to justify hiring such staff if cases are rare. Even at larger institutions, IT personnel who assist in sequestration typically have other primary IT responsibilities that may make coordination of sequestration activities difficult. The situation is further complicated by high turnover in the IT sector, as highly expert IT professionals seek more compensation than academic institutions can afford. Accordingly, in complex cases, or when there are on-going multiple inquiries/investigations, institutions may need to hire consultants to assist in the sequestration process, often at considerable cost. Further, as noted above, even this solution remains suboptimal.

What institutional policies, procedures, and guidelines have been effective in ensuring

successful sequestration?

As previously noted, many institutions have policies in place that make clear the institution's right of ownership in/and access to research data. These policies provide the underlying basis for all sequestration efforts.

Research misconduct policies mandated by 42 CFR 93.304 & .305 require policies/processes for sequestration of data at all institutions that conduct PHS-funded research. Some institutions also have more detailed standard procedures (SOPs) they follow in carrying out sequestration activities. [See, e.g., [University of Southern Maine, Procedure for Sequestration of Research Records](#); [Utah State University, Scientific Misconduct Procedures](#)].

In the experience of our member institutions, the primary determinants of sequestration success are the data management and retention practices within the individual research group. Thus, one of the best mechanisms to ensure successful sequestration is investment in efforts to promote a culture of research integrity and responsible conduct of research (RCR). Such investments also yield increased trust and collaboration between researchers and staff, which fosters both the reporting of research misconduct and the sequestration process itself.

What additions or changes are appropriate for [the ORI [sample Policies and Procedures for Research Misconduct](#)] to reflect the growing digital landscape, especially regarding sequestering digital evidence?

The current sample policies provide a broad outline for sequestration responsibilities. Given the wide variety of data encompassed by sequestration requirements, the most important consideration in making any changes to the sample policies is to avoid being overly prescriptive and instead preserve institutional flexibility in how sequestration should be addressed.

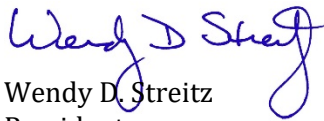
Prescriptive policies and procedures for digital sequestration impose a number of serious risks to the proper execution both of PHS-funded research and of the research misconduct review process. Specifically, increasing the cost, effort, and time required for sequestration will increase the already considerable time that it takes to conduct research misconduct proceedings and may not yield much in terms of benefit, given that institutions may make findings based on a preponderance of evidence. Further, process delays affect not only individual respondents, but also entire research groups, by negatively impacting reputations and the confidentiality of the process. Delays also can harm the ability of the research group to execute their responsibilities in relation to PHS-funded research, as well as damage the trust and collaboration between the researchers familiar with the data to be sequestered and the staff tasked with sequestration. Finally, for smaller institutions, or institutions that rarely process research misconduct cases, handling the logistics and expense of carrying out overly prescriptive sequestration practices may be unachievable.

One suggested addition to the sample *Policies and Procedures for Research Misconduct* is including in the section on the respondent's responsibilities a statement requiring the respondent to cooperate in sequestration efforts by assisting the RIO in identifying, locating and providing "all research records and evidence needed to conduct the research misconduct proceeding." [[42 CFR §93.305\(a\)](#)].

Increasingly researchers are developing and keeping their research data in digital format. Accordingly, processes to ensure the integrity of this data are paramount for research institutions, and similarly, strategies to ensure proper sequestration when this data is questioned are of utmost importance for the conduct of research misconduct proceedings.

We appreciate ORI's solicitation of stakeholders for information that should be considered in issuing any guidance in this area, and we hope that the information provided herein is useful to ORI. If you have any questions regarding these comments, please contact Kris West, Director of Research Ethics and Compliance, at kwest@cogr.edu.

Sincerely,

A handwritten signature in blue ink that reads "Wendy D. Streit". The signature is fluid and cursive, with the first letters of each word being capitalized and prominent.

Wendy D. Streit
President