# Duke University School of Medicine
# Department of Medicine
# Division of General Internal Medicine

OPERATING PROCEDURES FOR
SCIENCE CULTURE AND ACCOUNTABILITY
AND
DATA INTEGRITY AND SECURITY
2018

Table of Contents

# 1. Introduction

The following is taken from the Duke Department of Medicine website https://medicine.duke.edu/research/science-culture-and-accountability on Science Culture and Accountability.

The **Science Culture and Accountability Plan** (SCAP) outlines the expectations and recommendations for how the department, division and individual investigators can guarantee the responsible management and critical review of scientific data.

This plan, which details three levels of responsibility for promoting a culture that encourages responsible data management and produces data of the highest integrity — **individual, division and department** — also reflects these important principles:

- We foster an environment where scientific integrity is the highest priority.
- We emphasize high-quality, reproducible data and results.
- We value constructive critiques of research.
- We allow open discussion of any concerns regarding research conduct or integrity.

Each and every member of the Department of Medicine — faculty, trainees, staff and administrators — is expected to reflect and pursue these values. Ours is a shared commitment to the highest standards of scientific activity.

You can download the plan by going to the website and accessing the file stored on Duke Box with your NetID and password. It is also in Appendix 3.

To anonymously report a suspected compliance violation or concern, call the **Duke Compliance and Fraud Hotline** at 800-849-9793.

The **Duke Division of General Internal Medicine** (GIM) is committed to maintaining the highest quality and integrity of all its research data. GIM is committed to ensuring that policies and procedures are in place to reflect the highest professional conduct and to promote a culture in which scientific results are critically reviewed and accountability for data integrity is clearly delineated.

Our plan, as discussed in the Science Culture and Accountability Plan (DOM-SCAP), details the three levels of responsibility for promoting culture that encourages responsible data management and produces data of the highest integrity reflecting the important principles noted above.

Each member of the Division of General Internal Medicine (faculty, staff, administrators, fellows, students, trainees, volunteers, students, post-docs, or anyone who is or will be involved in IRB protocols) is expected to reflect and pursue these values.

This document has been developed to ensure the proper and secure handling of human subject research-related data, as well as administrative information related to research conducted in GIM. The purpose is to ensure that all data security measures, responsibilities and best practices are clearly delineated for GIM members.

All GIM personnel who are or will be involved in IRB protocols are required to review and sign this document prior to handling any research data within GIM. Personnel will demonstrate their commitment to the protection of human subjects and privacy by following the data security requirements stated in this standard operation procedure (SOP) manual. They must also follow all data security requirements listed in Duke University School of Medicine policies, including guidelines and trainings set by the Duke Office of Clinical Research (DOCR), the Institutional Review Board (IRB), and Federal and State regulations if applicable.

General Internal Medicine's Faculty Integrity Coordinator, Dr. L. Ebony Boulware, as well as the Integrity Officer, Tara Strigo, MPH, will be responsible for revising this document and disseminating it to GIM personnel. Any questions or concerns about research data management should be directed to them.

Dr. L. Ebony Boulware, Chief of General Internal Medicine, will confirm that each investigator is aware of the policies and various school, department and division resources that support researchers and their activities. Dr. Boulware will require that GIM faculty who are or will be involved in IRB protocols review and sign the GIM Science Culture and Accountability Plan when hired as well as during their annual updates.

All other GIM personnel who are or will be involved in IRB protocols will be required to review and sign the GIM Science Culture and Accountability Plan when hired as well as on an annual basis (at the time of performance evaluations, even if evaluations are not applicable for their position).

Dr. Boulware, along with Ms. Strigo, will verify the completion of the GIM Science Culture and Accountability Plan annually to ensure data integrity within GIM.

# 2. Responsibility for Ensuring Security Compliance

## 2.A. Overview

- The following is taken from the Duke Health Secure System Usage Memo https://intranet.dh.duke.edu/dhts/iso/SitePages/SSUM.aspx. GIM faculty and staff are required to review and comply with these policies.

Every member of the Duke Health workforce has a role to play in protecting the confidentiality, integrity, and availability of the valuable clinical and research data that Duke collects, produces, and maintains. The purpose of this memo is to provide you with an overview of the information security policies, standards, and procedures that apply to all Duke Health faculty, staff, students and affiliates. Your commitment to following the steps outlined in each of the sections below can help protect the personal information of our patients, their loved ones, and each other.

**Table of Contents (visit each site below for more information)**



**For More Information**
The Duke Health ISO intranet site provides additional information and advice on our security policies, standards, guidelines, and alerts. You can find the ISO site at Duke Health Information Security Office Intranet Site.
A complete list of our information security policies can be found at Duke Health Information Security Policies.
A complete list of our information security standards can found at Duke Health Information Security Standards.
If you have any additional information security questions or concerns that you would like to discuss, you can contact the ISO via email at security@.duke.edu.

- The following is taken from the Duke Data Security Policy at https://security.duke.edu/policies/data-security. GIM faculty and staff are required to review and comply with these policies. **(appendices/definitions referred to in this section can be found on the website noted above)**

**Authority**
Duke University Chief Information Officer
Duke Health Chief Information Officer
Duke University Chief Information Security Officer
Duke Health Chief Information Security Officer

**Purpose**

As stewards of Duke's resources, we are expected to exercise sound judgment using data prudently and ethically. Additionally, various federal and state laws impose obligations on Duke, including, but not limited to HIPAA, FERPA, FISMA, the NC Identity Theft Protection Act and PCI-DSS. Grants and contracts may impose requirements for the protection and preservation of associated data. As a result, it is important that all data (with appropriate priority given to Sensitive and Restricted data[1]), are reasonably and appropriately managed to maintain data integrity, availability, and when required, confidentiality to protect against accidental or unauthorized access, modification, disclosure and destruction.

Special consideration to research data is warranted, as some research data may be classified as public and open, while other research data may require greater protections due to the sensitivity of the data. This policy is not intended to impede the use or sharing of unrestricted (e.g. public) research data, but rather provide the framework for determining where controls are required for sensitive or protected research.

While every reasonable effort has been made to document the appropriate protections and responsibilities for data, it is possible that a specific case or issue may not be addressed or may raise a question. In such a case, the department or user is strongly encouraged to reach out to the appropriate security office (see Data Procedures section) for assistance determining the appropriate course of action.

[1] As defined in the Duke Data Classification Standard located at https://security.duke.edu/policies/data-classification-standard

**Policy**

### Data Classification

Each user is responsible for knowing Duke's data classification standard and the associated risks in order to understand how to classify and secure data. Duke data classifications are Sensitive, Restricted or Public. Sensitive data requires the highest level of security controls, followed by Restricted and then Public. A link to the Duke Data classification standard is provided in Appendix B.

### Data Access & Usage

Consistent with its classification, data shall be accessible to authorized users to fulfill their duties and responsibilities.

### Data Maintenance & Disposal

A user with authorized access to data will maintain the security (confidentiality, integrity and availability) of the data, consistent with Duke requirements. When Sensitive and Restricted data must be disposed of, to the extent permissible under law, that disposal must be in a manner that renders it unrecoverable. Only authorized services can be used for storage of Duke sensitive data; an approved list is available online: https://security.duke.edu/policies/duke-services-and-data-classification. Should you have questions about use of a service to store sensitive data, we encourage you to contact the Security Offices at security@duke.edu.

### Data Encryption

Sensitive data must be encrypted during network transmission, and if stored on mobile devices or removable media like a USB thumb drive. Any exceptions must be documented via a ServiceNow ticket and filed with the Duke IT Security Office or Duke Health Information Security Office for review. Additional information on encryption requirements for campus departments may be found at https://security.duke.edu/policies/encryption-standard, while additional guidance for Duke Health may be found here.

### Data Procedures

All Data Stewards at Duke must document their procedures, and other requirements that pertain to the security of the data for which they are responsible. This documentation must comply with all Duke

standards regarding data. The university Information Technology Security Office and Duke Health Information Security Office can be reached at security@duke.edu.

### Incidents

Any security incident or suspected security incident involving a Duke system, especially those containing Sensitive or Restricted data, must be reported immediately to the University IT Security Office or Duke Health Information Security Office, Data Manager and Data Steward, as applicable, pursuant to the incident management procedures referenced in Appendix B.

### Violations

Any violation of federal or state law, or this or other applicable policies, standards or contracts may result in corrective action up to and including dismissal/termination.

### Responsibilities

Set forth in Appendix A are typical responsibilities for the executive officers for Duke University and Duke Health, Data Stewards, Data Owners, Data Managers and users. An individual may fulfill the responsibilities of more than on position. Data stewards and data managers also qualify as users with regard to fulfilling their duties and responsibilities on behalf of Duke.

**Scope**
This policy is intended to safeguard all data, with priority given to Sensitive and Restricted data.

This policy applies to all trustees, senior officials, faculty, staff, students, subcontractors, or other persons who may have access to Duke data. See Definitions.

This policy applies to all data on Duke's communications resources, whether those resources are individually controlled, shared, stand-alone, or networked. It applies to all computers (including mobile devices) and communications facilities owned, leased, operated, or provided by Duke, or that are otherwise connected to Duke's communications resources. This policy also applies to all personally owned devices used to store, process, or transmit Duke data.

## 2.B. Division of General Internal Medicine (GIM)

### Principal Investigator

Principal Investigators of GIM projects have overall responsibility for data security related to the projects they oversee. This encompasses two primary areas:

- Training and oversight of all members of their research team(s)
- Project-level data security

### GIM Staff

GIM staff are defined as any research project staff or staff supporting the GIM mission including research staff, administrators, fellows, students, trainees, volunteers, students, post-docs.

### Data Security Team

The GIM Integrity Officer, Tara Strigo, MPH, along with the Faculty Integrity Coordinator, Dr. L. Ebony Boulware, is tasked with developing and implementing data security policies, providing examples/templates to GIM personnel, and assisting GIM staff and investigators in their use.

## 2.C. Duke University IT Security Office and Duke Health Information Security Office

### Duke University IT Security Office
**https://security.duke.edu**

The Duke University IT Security Office (ITSO) provides leadership in the development, delivery and maintenance of an information security and risk management program to safeguard the university's information assets and the supporting infrastructure against unauthorized use, disclosure, modification, damage or loss. The ITSO supports a comprehensive university-wide program that encompasses implementation of IT security methods and remediation, monitoring of IT security related events, threat and vulnerability management, and incident management. The ITSO collaborates with campus departments and business units on a wide variety of IT security-related issues and practices. Working with campus departments and the Duke Health System IT Security Office, we help manage risk and support secure, sustainable information technology services to meet the needs of the University.

**Objectives**

- Protect confidentiality, integrity and availability of university data.
- Promote a safe and secure information technology operational environment.
- Coordinate and communicate security related information to the University community.
- Identify and provide guidance on risk management, business continuity planning and compliance.

GIM faculty and staff are required to follow the policies and procedures set forth by ITSO listed at https://security.duke.edu/policies-procedures.

Our colleagues in the Duke Health Information Security Office (ISO) should be contacted via email at infosec@dm.duke.edu or see their site for any Duke Health System IT security issues.

### Duke Health Information Security Office
**https://intranet.dh.duke.edu/dhts/iso/SitePages/Home.aspx**

The Duke Health Information Security Office (ISO) is responsible for protecting information across all Duke Health entities, including Duke University Hospital, Durham Regional Hospital, Duke Raleigh Hospital, the Schools of Medicine and Nursing, research institutes, clinics, Health System corporate functions, and other related organizations. For more information:

A list of Frequently Asked Questions as well as multiple lists of additional resources are listed on the main page of their website.

A complete list of their information security policies can be found at Duke Health Information Security Policies.

A complete list of their information security standards can found at Duke Health Information Security Standards.

If you have any additional information security questions or concerns that you would like to discuss, you can email security@duke.edu.

# 3. Data Classification Standard

The following is taken from the Duke Data Classification Standard at https://security.duke.edu/policies/data-classification-standard. GIM faculty and staff are required to review and comply with these policies.
**(appendices/definitions referred to in this section can be found on the website noted above)**

**Purpose**

While performing their assignments at Duke University, all users will likely come into contact with many types of information or data, some of which may be considered Sensitive or Restricted according to Duke's data classifications and regulatory requirements. It is the responsibility of Duke to implement procedures and standards to help users protect their data.

The purpose of this standard is to define Duke's data classifications and data types for each classification. Please be aware that applicable federal and state statutes and regulations that guarantee either protection or accessibility of certain data records will take precedence over this standard. These regulations and laws include:

- FERPA (which protects many kinds of student educational data)
- HIPAA (which protects personal health information)
- HHS Title 45 CFR Part 46 - Protection of Human Subjects (which applies to research supported by a federal agency)
- NC GS 125-19 (which protects the privacy of library patrons' records)
- NC Identity Theft Prevention Act (which defines personal information and requires notification if a data breach occurs)
- PCI (which protects credit card holder information)

**Scope**

This standard applies to all data collected, stored, or processed by university staff or by third parties via contractual agreements with university departments or other organizational groups.

**Standards**

Data and Risk Classifications

To assist in handling information in any format, Duke as defined three classes of information: Sensitive, Restricted, and Public. Each classification tier requires a specific level of technical and procedural security controls due to the risk impact if the information is mishandled. These Technical Standards may be found at here.

Data that has not yet been classified should be considered Restricted until the Data Steward assigns the classification.

The classification of data is independent of its format. For example, if personal health information is revealed in a video recording of a lecture, then that video file should be classified as Sensitive. If paper credit card receipts are stored, then they should be classified as Sensitive.

Questions about classifying or handling the data should be directed to the Data Steward, your supervisor, your departmental security liaison, or the University IT Security Office. The departmental security liaisons, in coordination with the IT Security Office, can assist departmental users in developing appropriate controls and processes to protect Sensitive or Restricted data.

| Data Category & Risk | Definition & Access | Examples |
|---|---|---|
| Sensitive (High) | Sensitive data is the most restrictive data classification category and is reserved for data that Duke is either required by law to protect, or which Duke protects to mitigate institutional risk. Explicit institutional approval is | • Social Security numbers<br>• Credit Card numbers<br>• PHI (HIPAA -protected data)<br>• FERPA-protected data (non-directory information)<br>• Prospective student data |

| | | |
|---|---|---|
| | needed in order to receive access to Sensitive data. | • Donor data<br>• Contract data<br>• Financial data<br>• HR data<br>• Physical Plant details<br>• Research data<br>• Certain management information |
| Restricted (Medium) | Restricted information is the default data classification category. Restricted data is data that is not necessarily for public consumption, but also does not fit into the Sensitive category. Duke may have a proprietary obligation to protect Restricted data, but disclosure would not significantly harm the university. Access to Restricted data elements is determined by business process needs. | • Anything not Public or Sensitive<br>• Data that is restricted to specific groups<br>• Research detail that is not classified as Public or Sensitive<br>• Library transactions<br>• Financial transactions not including Sensitive data<br>• NDA data |
| Public (Low) | All other data, which can be accessible to the general public. Information that has been approved for publication, such as a press release or information published on www.duke.edu. (This does not include information that has been disclosed accidentally.) Access includes Duke University affiliates and general public. | • Public-facing websites<br>• Campus Maps<br>• FERPA directory data<br>• Faculty/Staff directory data<br>• Research data |

Roles and Responsibilities

To handle data properly, Duke faculty and staff need to be aware of the classification of a piece of information and the associated risks in order to understand how to properly and securely handle the information.

| Term | Definition |
|---|---|
| Data Steward | The individual who has accountability and executive authority to make decisions about a specific set of data. The Data Steward is the role of the person who is responsible for: the function that uses the information, determining the levels of protection for the information, making decisions about appropriate use of the information, classifying the information, and for the business results of the system or the business use of the information. |
| Data Manager | The persons who are responsible for implementing the controls the Data Steward identifies. The data managers are responsible for ensuring that the |

| | |
|---|---|
| | appropriate security controls are in place on systems containing Sensitive and Restricted data (see Technical standards). |
| Data Users | The persons who actually "touch" the information (enter, delete, even read). Users are responsible for taking reasonable precautions against disclosure of data they have access to. Users should not grant access to data without proper authorizations from the Data Steward. |
| Campus Units | It is the recommendation of the Duke University IT Security Office that all campus units that collect and store information document their policies, procedures, and architectures that pertain to collection and storage, regardless of the information format (electronic, paper, image, sound, etc.). This documentation should detail account creation and deletion, records retention and destruction, backup retention and destruction, and any other relevant procedures. |

Sensitive Server Registration

The University IT Security Office tracks servers containing Sensitive data. Campus units are asked to document which of their servers contain Sensitive and Restricted data, and update the ITSO on which systems contain Sensitive information.

Incident Reporting

Report the misuse or compromise of systems that handle, store, or propagate Sensitive data IMMEDIATELY to security@duke.edu.

# 4. Types of Data

Different types of data require different levels of security. In this section, five types of data sets are defined – identifiable, de-identified, limited, crosswalks and aggregate data.

## 4.A. Identifiable Data

The Health Insurance Portability and Accountability Act (HIPAA) privacy rule sets forth policies to protect all individually identifiable health information that is held or transmitted by a covered entity. These are the 18 HIPAA identifiers that are considered personally identifiable information. This information can be used to identify, contact, or locate a single person or can be used with other sources to identify a single individual. When personally identifiable information is used in conjunction with one's physical or mental health or conjunction, health care, or one's payment for that health care, it becomes Protected Health Information (PHI). items to be Protected Health Information (PHI)/Sensitive Information.

1. Name
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: a) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and b) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates related to an individual (including birthdate, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone number
5. Fax number

6. Electronic mail address
7. Social Security Number (SSN)
8. Medical record number
9. Health plan beneficiary number
10. Account number
11. Certificate/license number
12. Vehicle identifier and serial number, including license plate number
13. Device identifier and serial number
14. Web Universal Resource Locator (URL)
15. Internet Protocol (IP) address number
16. Biometric identifiers, including fingerprint and voiceprint
17. Full-face photographic images and any comparable images (Photographic images are not limited to images of the face)
18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification

If a communication contains any of these identifiers, or parts of the identifier, such as initials, the data is to be considered "identified". To be considered "de-identified", ALL of the 18 HIPAA Identifiers must be removed from the data set. This includes all dates, such as surgery dates, all voice recordings, and all photographic images.

Decedent Research: Be aware that the HIPAA privacy rule protects individually identifiable health information of deceased individuals for 50 years following the date of death. If the research will include any identifiers linked to living persons or involves accessing death records maintained by the State Registrars, local registrars, or county recorders, the project must be approved by the IRB in advance.

PHI shall be used solely for purposes related to the activities carried out by the research team per an IRB approved study protocol or preparatory to research.

## 4.B. De-Identified Data Set

**1. De-identification Certified by Statistician or Qualified Individual**

A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods or rendering information not individually identifiable accomplishes **both** of the following:

- Determines that the risk is very small that the information could be used, alone or in combination with other reasonable available information, by anticipated recipient to identify an individual who is a subject of the information; **and**
- Documents the methods and results of the analysis that justify such determination

**2. De-identification by removal of 18 Identifiers**

a. **All** of the above 18 identifiers of the individual or of relatives, employers, or household members of the individual must have been removed to qualify for exemption from the Privacy Rule (HIPAA).

b. The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

## 4.C. Limited Data Set (LDS)

A Limited Data Set (LDS) is described as health information that excludes certain, listed direct identifiers but that may include city; state; zip code; elements of date; and other numbers, characteristics, or codes not lists as direct identifiers. The direct identifiers listed in the Privacy Rule's limited data set provisions

apply both to information about the individual and to information about the individuals' relatives, employers, or household members. The following identifiers must be removed from health information if the data are to qualify as a limited data set:

1. Name
2. Postal address information, other than town or city, State, and zip code
3. Telephone number
4. Fax number
5. Electronic mail address
6. Social Security Numbers (SSN)
7. Medical record number
8. Health plan beneficiary number
9. Account number
10. Certificate/license number
11. Vehicle identifier and serial number, including license plate number
12. Device identifier and serial number
13. Web Universal Resource Locator (URL)
14. Internet Protocol (IP) address number
15. Biometric identifiers, including fingerprint and voiceprint
16. Full-face photographic images and any comparable images

An LDS may contain, for example:

- Dates of birth
- Dates of death
- Dates of service
- Town or city
- State
- Zip code

The difference between a LDS and de-identified information is that a LDS may not contain dates and certain geographic information associated with an individual that are absent from de-identified information.

A covered entity may use or disclose a LDS only for the purposes of research, public health, or health care operations.

### 4.D. Crosswalks

Data sets often include unique identifiers such as SSN's and study IDs. A crosswalk is a file that provides a mapping/match between different unique identifiers.

Special care must be made to protect crosswalks. A separate file would link study ID with actual SSN.

De-identified data sets often contain a newly created unique identifier completely separate from any identifying characteristics in the original study data sets. This created identifier is not capable of being translated so as to identify the individual. The only way for de-identified data to be re-identified is to be linked back to original data through a crosswalk, linking the created unique identifier with an established identifier.

It is essential to maintain crosswalks for de-identified data in case questions arise about the data or additional data is requested. However, the crosswalk file cannot be accessible to the recipient of de-identified data, as this would make the data identifiable.

### 4.E. Aggregate Data

Aggregate or summary data are the result of combining information that meets specific criteria. By definition, aggregate or summary data are the product of combining two or more data items. A purpose is to present meaningful data about multiple individuals or facilities without revealing sufficient information from which the identity of an individual or site can be deduced. A series or "string" of data elements regarding an individual case, even if all or most identifiers are removed such as in de-identified or limited data sets, are case-specific data and not aggregate or summary data.

Examples of aggregate or summary data are the number of study participants who have diabetes, the percent of study participants who were screened for colorectal cancer, and the average number of surgeries performed at Duke University Medical Center in a given time period. Meeting presentations, abstracts, published articles, and study reports typically contain aggregate or summary data in the form of tables, figures, and charts.

Responsibilities

**PI:** The PI is responsible for ensuring that all identifiable data related to their projects are protected according to HIPAA standards. The PI is responsible for working with project statisticians (and other project staff members, if relevant) to ensure that any identifiers are properly removed from any de-identified or limited data sets related to the projects they oversee. The PI is also responsible for ensuring that crosswalk files are securely maintained.

## 5. Access to Data

An essential part of data security is controlling access to data. A project's data collection methodology should be described in detail in its IRB-approved protocol.

Each Principal Investigator (PI) is provided an electronic folder for their research project on the Duke GIM secure server. Folders are created by Duke Health Technology Solutions (DHTS) with permissions for access. Only IRB approved research project staff who need access to the study database (e.g. Clinical Research Coordinator (Sr), Clinical Research Specialist (Sr), Statistician, Fellow, Student) and related files in this folder, are granted access by DHTS. Individuals must be listed on the IRB staff listing before they are granted access. DHTS can create multiple folders within the main folder and assign access based on staff roles and responsibilities. For example, only the Statisticians can be granted access to the analysis folder. The PI or Clinical Research Coordinator/Lead Research Staff can request DHTS create a new secure folder on the GIM server, request permissions for an existing user such as access to specific folders; request removal permissions for existing users, and request restrictions to specific folders; and grant VPN or/or access to an IRB approved user external to Duke so that secure data can be accessed outside of the Duke Health network.

For internal and external release of data, the PI must obtain approval by the IRB and follow their guidelines for release.

Responsibilities:

**PI:** The PI is responsible for ensuring that project generated data are used, stored, and shared appropriately. The PI is also responsible for ensuring that all access to data sets are obtained by project staff in accordance with an IRB-approved protocol.

**PI and Clinical Research Coordinator/Lead Research Staff:** The PI and Clinical Research Coordinator/Lead Research Staff are responsible for ensuring that project-specific guidelines regarding data access are documented in IRB-approved protocols. They are also responsible for ensuring that project-specific data access is restricted to appropriate individuals on the research team, and that these individuals are appropriately credentialed, trained, and supervised.

**PI and Clinical Research Coordinator/Lead Research Staff:** The PI and Clinical Research Coordinator/Lead Research Staff are responsible for working with project statisticians to ensure that all project data sharing adheres to the processes described and approved by the IRB. This includes ensuring that IRB-approved protocols describe any plans for data sharing (including identifiable information, limited data sets, and/or de-identified data) and that this information is kept updated with the IRB if/whenever modifications are made. This also includes ensuring that staff listings are updated as needed.

## 6. Data Documentation

GIM has a strict policy that all staff, faculty, or affiliated research investigators adhere to the very highest standards for data collection and data entry. GIM requires that Principal Investigators conducting IRB approved research along with their project staff engaged in data collection and data entry understand the importance of documenting raw data exactly as it is collected with zero manipulation, alteration, or falsification.

The agreement outlines the following Core Principles of Data Entry and Documentation:

- All staff engaged in data collection or data entry must have all requisite IRB training and must be already approved by IRB as a study team member before any data collection or data entry can occur.
- All staff engaged in data collection or data entry will receive formal training on how to collect data and enter it.
- Staff will be informed that they will be observed during the process of data collection (PI and Clinical Research Coordinator/Lead Research Staff responsible).
- Staff will be informed that the data will be periodically spot-checked without warning (PI responsible).
- Staff will be informed that evidence of data manipulation, alteration, or falsification will be the basis for immediate termination of employment.

GIM recommends minimal use of paper-based data entry forms whenever possible, due to added possibility of human error when transferring data from paper to electronic media. All research projects are encouraged to use an electronic database for direct entry of raw data when possible. Data capture programs should ideally contain safeguards (e.g., 'logic rules') to protect against erroneous data entry when possible. Duke REDCap (Research Electronic Data Capture) is a suitable tool for data collection. The Duke Office of Clinical Research (DOCR) is used as a central location for data processing and management. REDCap is a software toolset and workflow methodology for electronic collection and management of research and clinical trial data. REDCap data collection projects rely on a thorough study-specific data dictionary defined in an iterative self-documenting process by all members of the research team with planning assistance from the DOCR. This iterative development and testing process provides a well-planned data collection strategy for individual studies. REDCap provides a secure, web-based application that is flexible enough to be used for a variety of types of research, provide an intuitive interface for users to enter data and have real time validation rules (with automated data type and range checks) at the time of entry. These systems offer easy data manipulation with audit trails and reporting for reporting, monitoring and querying patient records, and an automated export mechanism to common statistical packages (SPSS, SAS, Stata, R/S-Plus). Data from DOCR can be downloaded to the GIM secure server and combined with other data from, for example, tracking databases, claims data, etc.

All studies should store the original raw data on the GIM secure server. For all data stored on the GIM secure server, original raw data files are stored within the PI's project specific folder with limited access to the PI and Clinical Research Coordinator/Lead Research Staff. Statisticians working on the research project are given access to their own folder with limited access within the PI's project specific folder. The statistician(s) will review the data, recode if necessary, create new variables, write all measures (or scales) scoring programs, create finalized datasets that are then used for analyses, and save the files in this folder.

The Duke Department of Biostatistics and Bioinformatics (B&B) provides support for GIM faculty research. The Department of B&B assigns a team of statisticians (e.g., PhD/masters) to work together on all studies. Team members are expected to review each other's work for quality assurance and control. As a standard in the department, new staff members, as well as annually for all staff, discuss "good practices" for data documentation and follow the guidelines listed below. GIM supports and follows these guidelines as well.

- Have a clear folder structure.
- Establish a clean database/file that is not to be modified. This is the starting or source point for a possible audit. Access this data for each new analysis but construct analysis databases/files.
- Use Statistical Analysis Plans (SAPs) to document and track work. Clearly comment and document all programs. A non-team member should be able to follow the work from result back to the source data. Analysis variables such as recodes and summary scores should be documented in the SAP. Statistical code depends on the language used but all should include good comments, a proper header, and a log.
- When possible, independent analyst check PI analyses.

- Include a date and time on all files/reports.
- Analysis guidelines are typically dictated by the regulator body or journal. (Recommendations can be found in The Annals of Medicine.)
- Here are other references staff are encouraged to review:
    - Thomas L, Peterson ED. The Value of Statistical Analysis Plans in Observational Research: Defining High-Quality Research From the Start. JAMA. 2012;308(8):773-774. doi:10.1001/jama.2012.9502.
    - Galili T. Managing a Statistical Analysis Project - Guidelines and Best Practices. R-bloggers 2010. http://www.r-bloggers.com/managing-a-statistical-analysis-project-%E2%80%93-guidelines-and-best-practices/
    - http://stats.stackexchange.com/questions/2910/how-to-efficiently-manage-a-statistical-analysis-project
    - Hadley Wickham offers a comprehensive overview of R project management, including *reproducible exemplification* and a *unified philosophy of data*.
    - In R-oriented Workflow of statistical data analysis, Oliver Kirchkamp offers a very detailed overview of why adopting and obeying a specific workflow will help statisticians collaborate with each other, while ensuring data integrity and reproducibility of results. It further includes some discussion of using a weaving and version control system.
    - Stata users might find J. Scott Long's, The Workflow of Data Analysis Using Stata, useful.

Responsibilities:

**PI and Project Staff:** The PI and project staff are responsible for taking Duke required/suggested trainings for data documentation, integrity and security. The PI is responsible for ensuring their staff has taken the required/suggested classes prior to being given access to data.

**PI and Project Staff:** The PI and project staff are responsible for documenting raw data exactly as it is collected with zero manipulation, alteration, or falsification. Any concerns should be reported to the PI or the GIM Faculty Integrity Coordinator or Integrity Officer.

**PI and Clinical Research Coordinator/Lead Research Staff:** The PI and Clinical Research Coordinator/Lead Research Staff are responsible for observing staff during data collection process.

**PI:** The PI will periodically spot-check the data.

# 7. Duke Health Secure System Usage

Every member of the Duke Health workforce has a role to play in protecting the confidentiality, integrity, and availability of the valuable clinical and research data that Duke collects, produces, and maintains. The purpose of this website (https://intranet.dh.duke.edu/dhts/iso/SitePages/SSUM.aspx) is to provide you with an overview of the information security policies, standards, and procedures that apply to all Duke Health faculty, staff, students, and affiliates. Your commitment to following the steps outlined in each of the sections below and online can help protect the personal information of our patients, their loved ones, and each other.

## 7.A. GIM Environment

The GIM computing environment consists of Dell, Lenovo, and Apple desktops and laptops. All machines are running a minimum of Windows 7/OSX10.6 or higher. All machines are licensed to run Office and Symantec Anti-Virus. Per Duke policy, all laptops are to be encrypted with either Bitlocker on PC or Filevault. Mobile devices used to connect to the secure Duke Health wireless network or to access Duke Health resources are required to enroll in Duke Health Mobile Device Manager and must install AirWatch (https://mobile.dhts.duke.edu/message-duke-health-leadership) on their device.

## 7.B. Protecting Data Storage, Transmission, and Backups

Research data collected from Duke Health under an IRB-approved protocol must be stored on Duke Health managed servers, not Duke University, VA or any other third-party servers, unless (a) it has been fully de-

identified or anonymized, (b) outlined in an informed consent, or (c) a Data Transfer Agreement has been put in place to allow the third party to receive that data.

The information below is taken from the latest Duke Health Secure Systems Usage Memo: https://security.duke.edu/sites/default/files/atoms/files/DukeMed_SSUM_2016.pdf

- Except for explicitly approved uses such as receiving Duke Health email on personal smartphone or tablet, do not store Duke SEI on non-Duke owned systems or devices, such as personal computers at home.
- PHI and other SEI that has been approved for storage on mobile devices or removable media (e.g. portable hard drives, memory sticks, flash drives, CD/DVDs, etc.) must be encrypted in accordance with the Duke Health Mobile Computing and Storage Device Standard.
- Use of file sharing or cloud-based services for data containing SEI (e.g. Dropbox, SkyDrive, Google Drive, etc.) is not allowed without prior approval from the Duke Health ISO. Duke is working to provide an alternative solution for this type of service, and it will be announced when available.
- Clinical data may not be shared with vendors or other third parties who perform services on behalf of Duke unless there is a Business Associate Agreement (BAA) and Data Security Agreement (DSA) in place with the organization that would be receiving the data. If there are any questions about whether there is a BAA or DSA in place, you may contact Duke Procurement Services. BAAs and DSAs must be reviewed and approved through Procurement's processes, and may only be signed by Procurement.
- Research data collected from Duke Health clinical activities under an IRB-approved protocol must be stored on Duke Health managed servers, not Duke University, VA or any other third party servers, unless (a) it has been fully de-identified or anonymized, (b) outlined in an informed consent, or (c) a Data Transfer Agreement has been put in place to allow the third party to receive that data.
- When sending clinical data, research data, or other SEI outside of the Duke Health network, SSL-encrypted protocols such as HTTPS, SFTP, or SCP must always be used.
- User devices, including workstations, laptops, and other mobile devices, are generally not backed up. Any data stored on a user device may be permanently lost in case of a system failure or the loss of the device. Instead, store data on Duke Health servers through network shared drives.
- Dispose of all old storage media, including but not limited to hard drives and backup tapes in accordance with the Duke Health Media Control Standard.
- External data recovery services (e.g. to recover data from failed hard drives) may not be used unless there is a BAA in place with the vendor.
- If you have any questions about how to securely store, manage, or transfer data, please contact your IT support group or the Duke Health ISO for assistance.

## 7.C. Protecting Workstations and Laptops

Research data within GIM are required to be stored on the GIM secure server which has daily backup. Identifiable data should not be stored on individual laptops or other storage devices. Duke laptops must be encrypted by DHTS. You must contact DHTS to completely clean/wipe out old desktop/laptop computers before sending them to surplus.

The information below is taken from the latest Duke Health Secure Systems Usage Memo: https://security.duke.edu/sites/default/files/atoms/files/DukeMed_SSUM_2016.pdf

- Never uninstall or alter the configuration or operation of any systems management agent or anti-virus software that is installed on your Duke workstation or laptop.
- Discontinue use of any system that shows signs of being infected by a computer virus (also referred to as malware). See the "Recognizing and Reporting Security Incidents" section below for more information.
- Arrange computer monitors so that, as much as possible, they are facing only the individual using them. If available to you, consider the use of screen filters to limit visibility to those directly in front of the screen. You are responsible for ensuring that unauthorized individuals are not able to view your screen.
- Log off or lock your workstation or laptop if leaving the system unattended. Screen locks should be configured to automatically lock a screen after a maximum of 15 minutes, and requiring that your password be entered to unlock the screen.
- Per Duke Health policy, all laptops must be fully encrypted using an ISO-approved solution, unless the Chief Information Security Officer (CISO) has granted an exception. Currently, Symantec PGP and

Apple's FileVault 2 are the two approved solutions. Contact your IT support group for assistance with encrypting a laptop.

- Ensure that laptops are stored in secure locations when unattended. If possible, never leave them in a car, and if you must, place them in a locked hidden location, like a trunk.
- Provisions for installing hardware or software on workstations and laptops:
    - **If your workstation or laptop is used to conduct work under a Federal contract or Medicare Shared Savings Program (MSSP) which requires FISMA compliance**, you may not install software, hardware, or otherwise change the configuration of your workstation or laptop without explicit approval from your IT support group. **Failure to do so may place Duke out of compliance with federal contract requirements**.
    - For all other workstations and laptops, extreme caution should be used when installing any new hardware or software. It is recommended that you contact your local IT support group for assistance in making any hardware or software changes to your system.

## 7.D. Protecting Mobile Devices

The information below is taken from the latest Duke Health Secure Systems Usage Memo: https://security.duke.edu/sites/default/files/atoms/files/DukeMed_SSUM_2016.pdf

- When connecting your mobile device to Duke Health's email system, a basic set of security controls will be enforced on your device. These include the following:
    - Requiring the use of a passcode to lock the device when it is idle for more than three minutes. Numeric passcodes are the minimum requirement; alphanumeric are recommended. A password history is maintained to prevent the successive re-use of passcodes.
    - Automatically wiping the device after ten successive failed attempts to use a passcode to unlock the device.
    - Encryption is enabled on the device and for any external storage cards (e.g. SD Cards) on Android devices.
- You are responsible for applying software updates to your device and any installed applications as soon as practical after being made available by the vendor.
- **Do not "jail break" or "root" your device**. Doing so disables basic security controls on the device, and increases the chance of a malware infection.
- Only install apps from legitimate sources, such as the Apple App Store or Google Play.
- If your device has been lost or stolen, please note that Duke Health reserves the right to remotely wipe the device to prevent the loss of PHI.

**Duke Health Mobile Device Manager**

Mobile devices used to connect to the secure Duke Health wireless network or to access Duke Health resources are required to enroll in Duke Health Mobile Device Manager and must install AirWatch (https://mobile.dhts.duke.edu/message-duke-health-leadership) on their device. This is required for the following groups:

- Anyone who carries a Duke-owned device; this includes smartphones and tablets.
- Anyone that receives a stipend for use of their own mobile device.
- And anyone that brings their device to work for personal use and accesses our secure wireless network.

This is the only way you to access Duke's secure wireless network and view Duke email via a mobile device

## 7.E. Electronic Communications

The information below is taken from the latest Duke Health Secure Systems Usage Memo: https://security.duke.edu/sites/default/files/atoms/files/DukeMed_SSUM_2016.pdf

- Email containing SEI that is sent outside of Duke Health must be sent using the Secure Email feature in the Duke E-mail system. This may be done using the "Sensitive Electronic Information" button in Outlook, or if that is not available in your email client, by placing the text "(secure)" at the beginning of the Subject line of your email. For more information on using Secure Email, see the Duke Health Secure e-Mail.

- Only use a Duke Health approved email system for Duke Health communications. Currently approved email systems include the Duke Health Exchange server and Duke's Microsoft Office 365 email solution. **Personal email accounts through services such Gmail, Yahoo, and Hotmail, or external sites that aggregate email accounts, may not be used to conduct Duke Health business.**
- Duke Health email containing PHI or SEI may not be forwarded to a non-Duke Health email account.
- The Duke Health Electronic Communications Policy provides further requirements for securing electronic communications, including faxing and text paging.
- The Duke Health Social Media Policy provides the policies and guidelines for the appropriate and secure use of social media sites such as Facebook, Twitter, and others. PHI must never be posted on social media sites, including online forums provided by Duke unless they have been specifically approved for PHI.
- Extreme caution must be used with photography and videography inside of clinical facilities to prevent inadvertent disclosures of PHI. Please refer to the Photographing/Videotaping/Audiotaping of Patients policy.

## 7.F. Physical Security

Any hardcopy forms containing PHI (consent forms, surveys, etc.) must be kept secure in accordance with the research study's IRB-approved protocol.

The information below is taken from the latest Duke Health Secure Systems Usage Memo: https://security.duke.edu/sites/default/files/atoms/files/DukeMed_SSUM_2016.pdf

- Retrieve printed sensitive information immediately upon printing. When disposing of hardcopy, use bins that have been marked for the disposal of confidential documents. If those are not available, use a crosscut shredder.
- Report unauthorized or unknown people that appear in non-public areas to a manager or facilities security officer.
- In areas that require badge access, do not allow others to follow you through a door without badging in.

## 7.G. Passwords and Accounts

All Duke personnel must have their own user account for access to any computing system. The user's login name and password must never be given to or shared with any other individual for any reason.

To maintain optimal security and data protections employees of GIM should log off or activate password protection (lock workstation) at the desktop/laptop every time they leave their workstations. Workstation locking will be accomplished manually or through an automatic timer. Each workstation/laptop will have a password protected screen saver with a time out setting. Users should completely log off and restart all computers every workday and must practice due diligence to ensure all rooms containing computers are secured properly (for example, locking when leaving if there is a lock on door).

Upon termination of a research project and/or employment, the GIM employee/student and his/her supervisor have the responsibility of notifying the GIM DHTS contact. Access to the GIM server will be disabled upon termination. Account information (such as email, electronic files, voice mail, and other date) will not be made available to a 3rd party except in rare cases as defined in the Duke Acceptable Use Policy described on the ITSO Website at https://security.duke.edu/policies/acceptable-use.

- Strong passwords must be used to secure access to critical systems and data. A single compromised password can lead to a significant data breach. Duke Health relies upon you to protect your passwords at all times.
- Everyone using Duke Health IT resources must create and use passwords that comply with the Duke Health Password Standard.
- Passwords must be changed at a minimum of every 180 days. All faculty/staff should receive automated reminders several days prior to their password's expiration.
- Your Duke passwords are never to be shared with another individual, including Service Desk staff and administrative assistants. Doing so is a breach of policy and can result in disciplinary action.
- Never use your Duke password on a non-Duke system (e.g. for personal email, banking, or social media site).

- Avoid writing your passwords on paper (e.g. sticky / post-it notes). If you need assistance remembering and managing your passwords, Duke has licensed the LastPass utility, which can be used to generate strong passwords and store them in a secure fashion. For more information, see the LastPass FAQ.

### 7.H. GIM Secure Server Backup

The Duke Division of General Internal Medicine (GIM) secure server is maintained by Duke Health Technology Solutions (DHTS).

Short term Backup:
Data stored on \\duhsnas-pri\dudom_gim\Private will be backed up via Isilon snapshot every ~6 hours. These snapshots allow the user to restore previous versions (within the prior 30 days) of a file/folder in the event of data loss.

Long term Archival:
Data stored on \\duhsnas-pri\dudom_gim\Private will be backed up to \\duhsnas-pri\dudom_GIM_archive using the Retrospect Backup Software hosted on an Enterprise Virtual Machine. The archive data will be stored in a proprietary, compressed, and journaled file format readable only by the Retrospect Software.

A task will be scheduled to backup once every month with the archive being retained for a minimum of 7 years. Data restores can be requested by submitting a ticket detailing the file/folder name, and approximate date of restore needed.

\\duhsnas-pri\dudom_GIM_archive and the machine hosting Retrospect will be secured to only allow access to only Academic Support Team Leads.

Archival files also benefit from the Isilon 6 hour/30 day Snapshot system, for a third level of protection.
DHTS IT Analyst: Aby Conaway
Aby.conaway@duke.edu
919-668-9046

Responsibilities**:**

**PI and Project Staff:** The PI and project staff are responsible for communicating with DHTS personnel regarding secure system usage, data storage transmission and verification of back up, protecting workstations and laptops, protecting mobile devices, electronic communications, physical security, passwords and accounts, and data protections.

## 8. Data Transmission

### 8.A. Shared Network Folders

Shared network folders can be used by GIM personnel to make files available to other GIM personnel. If access to an IRB-approved project is required, the project PI verifies the user is noted on the staff listing for that particular project. Shared folders also can be used to hold information for non-GIM personnel to access specific GIM files with proper authorization. For example, DHTS personnel can give access to temporary shared folders to an IRB-approved study co-investigator or research staff at another research facility to retrieve specific files. These co-investigators and research staff must have IRB-approval with documented training. If external to Duke, they will also need to have a temporary Duke account. Contact the GIM Administrative Assistant, Iris Harris, for assistance with requesting a Duke account for external Duke researchers.

### 8.B. Facsimile (Fax) Machines

Fax equipment is located in a secure and/or protected area away from unauthorized people. Employees should only transmit individually-identifiable information via facsimile (fax) when no other means exist to provide the requested information in a reasonable manner or timeframe.

Prior to faxing PHI or medical record information, it is necessary to call the recipient to confirm the receiving fax machine is in a secure location or the recipient is available to retrieve the fax immediately.

### 8.C. Telephone Contacts

GIM personnel may leave voice-mail messages for research participants on answering machines following IRB rules and an IRB-approved protocol.

## 9. Annual Compliance

All GIM personnel must review and sign all required forms in this SOP document and be in compliance with all requirements mandated by the Duke University Medical Center, Duke Office of Clinical Research, and IRB. GIM server access will be suspended if any of these requirements (e.g., completion of mandatory training courses) have not been met.

### 9.A. Mandatory Training

All Duke staff are required to sign the Duke Confidentiality Agreement when hired. A copy of this form should be retained in the staff member's department file. The agreement is available on the HR website at https://hr.duke.edu/forms/confidentiality-agreement.

All GIM personnel involved in research must complete the following relevant training courses which can be found with their links below:

**Duke University Health System Institutional Review Board (IRB)**
(https://irb.duhs.duke.edu/training-and-education)

- Collaborative Institutional Training Initiative (CITI) (https://www.citiprogram.org)
  (Select Duke Health)
  Biomedical Research (Basic Cource – refresher every 3 years)
  Good Clinical Practice (GCP) (every 3 years)
  Research with children (once)
  Research with prisoners (once)
  Research with pregnant women/fetuses (once)

**Responsible Conduct of Research (RCR)**
(https://medschool.duke.edu/RCR) (every 3 years)

**Duke Office of Clinical Research (DOCR)** https://medschool.duke.edu/research/clinical-and-translational-research/duke-office-clinical-research/policies-training-and-0

- Trainings listed are optional, however, **Investigator Responsibilities** and **Adverse Events** are **recommended for PIs**.
- Classes titled **Developing the Informed Consent Form** and **Screening and Consenting Subjects** are for any person participating in the Development of the Informed Consent Form and/or Screening and Consenting Subjects and is **required** for PIs and project staff (either or both classes) before participating in any aspect of the Informed Consent Process within 120 days of hire.

**Research Costing Compliance** (http://finance.duke.edu/research/training/index.php?crs=307&trn=26)
Required for PIs when hired and as module as updated

**Duke University and Duke Medicine Occupational & Environmental Safety Office** (www.safety.duke.edu)

- Compliance training (HIPAA) (annually)
- Fire/Life Safety (annually)
- Influenza Policy Compliance
- Tuberculosis (TB) Safety Training
- Others as determined by your position (will be included on the site when you log in)

Responsibilities:

**PI and Clinical Research Coordinator/Lead Research Staff:** The PI and Clinical Research Coordinator/Lead Research Staff must ensure that he/she and all project staff have completed all mandatory training within the deadlines and are on the IRB approved protocol prior to handling any data on projects they oversee.

**Project Staff:** All project staff are required to complete all trainings within the deadlines prior to handling any data on projects.

## 10. Recognizing and Reporting Security Incidents

The following policies are found on https://intranet.dh.duke.edu/dhts/iso/SitePages/SSUM.aspx:

- A security incident is an event that may result in the confidentiality, integrity, or availability of Duke Health information systems or data being compromised. Indications of a security incident may include the following:
  - The intentional or unintentional misuse of (a) patient information, (b) information pertaining to Duke Health faculty, faculty, or students, (c) Duke Health computer systems, or (d) other information that is classified as sensitive or restricted by Duke's Data Classification Standard.
  - Theft or loss of a computer or mobile device (e.g. smartphone or tablet) that is either owned by Duke or possibly stored or had access to Duke Health patient information or other sensitive data.
  - Observing odd behavior or other signs that a computer may have been infected with malware or otherwise compromised by an intruder.
  - Clicking on a link or opening an attachment in a suspicious email.
  - Finding evidence that a Duke Health system, application, or data set may have been modified or accessed without authorization.
  - Storing patient information or other sensitive data in an insecure manner on a workstation, computer media (e.g. flash drive or CD/DVD), or unauthorized web site (e.g. file sharing sites such as DropBox).
  - Leaving printed output containing patient information or other sensitive data in a location where unauthorized individuals may view it.
  - If you suspect someone knows your password, your last date and time noted on the login screen is not correct, or your account has been locked out.
  - Faxing, mailing, or emailing patient information or other sensitive data to an incorrect phone number or address.
- If you believe that you have observed an information security incident, please take the following steps:
  - Report the incident immediately to the DHTS Service Desk by calling 919-684-2243 or online at https://duke.service-now.com.
  - If the incident involves your computer: Discontinue using it until the Duke Health Information Security Office has evaluated the situation.
  - If the incident involves the loss or theft of a computer or mobile device: In addition to reporting the incident to the Duke Health Service Desk, file a report with the Duke University Police Department, which can be reached at 919-684-2444. For further information, refer to the Lost or Stolen Device Procedure (download the form from the website above).

## 11. IRB Approval

The Duke University Health System Institutional Review Board (DUHS IRB) has responsibility for the review of research involving human subjects for the Duke University Schools of Medicine and Nursing, Duke Regional Hospital (formerly Durham Regional Hospital), Duke Raleigh Hospital, and Duke Primary Care. For all activities related to research involving human subjects, an IRB protocol must be submitted for IRB review for approval or exemption. (http://irb.duhs.duke.edu)

## 12. Faculty Meetings

### 12.A. Research Faculty

GIM requires research faculty attend faculty meetings for discussion of research integrity including:

1. How to ensure data integrity
2. Creation and saving of analysis plans
3. Tracing analyses and potential double-checks for validity
4. Preparing for an audit
5. Management of research staff to ensure data integrity
6. Discussion of other research announcements

In addition, research faculty will be required to present their research in progress in a GIM forum (VA HSRD, DCRI Comparative Effectiveness, CKD Clinical and Health Policy Forum, Fellow and Faculty Works in Progress)

### 12.B. Early Career Faculty

Mentees will participate in a weekly 1-hr training course designed to provide in-depth coverage of research, teaching/mentoring, and leadership skills needed to be a successful independent researcher in academic medicine. This curriculum is overseen by Dr. Edelman but involves instruction from many faculty within and outside the DGIM. The sessions will be discussion-oriented, with a faculty member present to facilitate conversation.

Junior Faculty need training in presentation, and ongoing evaluation of the quality and direction of their work. Therefore, most sessions will be Works in Progress (WIP) presentations done by the Junior Faculty members (and invited fellows from DGIM or the Durham VAMC Center for Innovation in Primary Care). Each Junior Faculty member will present twice in an academic year. In the WIP sessions, mentees will present preliminary research findings; grant ideas; review an abstract prior to submission to a meeting; or receive feedback on presentation skills via a practice talk for a conference. Mentees have latitude to decide to use the session to benefit him/her the most.

In week 4 of each month, topical meetings will be held that address the research skills needed to be a successful independent researcher (Table 2); these will be facilitated by a DGIM faculty member. Early career faculty will attend meetings for at least the first years of their faculty appointment. Thereafter, faculty should consult with the Division Chief about recommendations for continued participation. Different speakers will be sought each year so that the specific content discussed under each topic will evolve.

### 12.C. Clinical Research Coordinator/Lead Research Staff

GIM Director of Research/Integrity Officer, Tara Strigo, leads the GIM Research Leadership Meetings. These meetings are a forum for all Clinical Research Coordinators and other Lead Research Staff to discuss Duke-related issues. The meetings are held once a month and include general GIM updates, discussions on grant-related issues, IRB-related issues, new/revised Duke, DOCR, DOM CRU policies and requirements, etc. Guest speakers from Duke are invited as needed.

## 13. Internal Audits/Reviews

The following is taken from the 07/15/2015 Duke Medicine Memo: Quality Assurance Monitoring Review Standards for Clinical Research.

**Policy**

The Duke School of Medicine CRUs or Oversight Organizations will be responsible for internal reviews of clinical research studies conducted by Principal Investigators (PIs) within their unit or organization. Periodic internal reviews are required to ensure the safety of research subjects and to verify the study is conducted, recorded, and reported according to protocol, standard operating procedures, GCP and applicable regulatory requirement(s). Internal reviews are conducted independent of monitoring visits by study sponsors. The studies prioritized for review should be high-risk, prospective studies that consent subjects. CRUs with multiple divisions should select studies for review from each of their divisions. It is expected that each CRU will perform a minimum of 12 quality assurance monitoring reviews per year; smaller CRUs or Oversight Organizations may not attain this level of reviews based on the risk criteria listed below. Reviews may be conducted remotely, provided all required records are available.

**Study Selection/Assessing Risk**

Each CRU or Oversight Organization will prioritize studies for review utilizing the following criteria. Higher priority will be given to studies that meet multiple criteria. A risk assessment tool will be provided in REDCap.

- Studies utilizing investigational drugs, devices, or procedures where the IND or IDE is held by a Duke investigator
- Federally-funded studies
- Studies without an external monitor
- Studies being conducted by a new PI

**GIM Reviews**

GIM may also conduct random reviews of IRB-approved research studies within the division. This peer-review may be conducted post IRB approval and prior to recruitment (if applicable) or analysis of data if no participants are recruited. The review would focus on regulatory documentation, consent process, study documentation, data security and integrity and review of participant payment process, if applicable. Reviews would be conducted by the GIM Director of Research/Integrity Officer, Tara Strigo.

## 14. Available Resources and Reporting Mechanisms for Scientific Accountability

- The NIH Office of Research Integrity (https://ori.hhs.gov)
- Guidelines for the Proper Handling of Digital Image Data (http://jcb.rupress.org/content/166/1/11.full)
- Online Learning Tool for Research Integrity and Image Processing (http://ori.hhs.gov/education/products/RIandImages/default.html)
- The Compliance and Fraud Hotline: To anonymously report a suspected compliance violation or concern, the Compliance and Fraud Hotline at Duke is at 800-849-9793

# APPENDIX 1
# Duke Division of General Internal Medicine Science Culture and Accountability Plan Checklist for Faculty & Checklist for Research Staff

## Science Culture and Accountability Plan

## GIM Checklist for Faculty

The **Duke Division of General Internal Medicine** (GIM) is committed to maintaining the highest quality and integrity of all its research data. GIM is committed to ensuring that policies and procedures are in place to reflect the highest professional conduct and to promote a culture in which scientific results are critically reviewed and accountability for data integrity is clearly delineated.

Each member of the Division of General Internal Medicine (faculty, staff, administrators, fellows, students, trainees, volunteers, students, post-docs, or anyone who is or will be involved in IRB protocols) is expected to reflect and pursue these values.

These documents have been developed to ensure the proper and secure handling of human subject research-related data, as well as administrative information related to research conducted in GIM. The purpose is to ensure that all data security measures, responsibilities and best practices are clearly delineated for GIM members.

All GIM personnel who are or will be involved in IRB protocols are required to review and complete these document prior to handling any research data within GIM.

**Indicate with a Y for Yes or N for No for each item.**

____ I ensure that I, and my research staff engaged in scientific research, have reviewed this SOP document.

____ I ensure that I, and my research staff engaged in scientific research, have completed all required institutional training modules related to responsible data management and have taken advantage of programs offered through the SOM that are designed to address research integrity.

____ I have ensured that all my research project(s) have implemented and maintained policies for responsible data management within my research groups.

____ I have established mechanisms by which the validity and integrity of critical data generated by my research can be confirmed.

____ I, as well as my research staff, have completed the Data Integrity and Security class presented by DOCR. (this is a 1 time only class, but verify all existing and new staff have taken)

____ I, as well as my research staff, have signed the required Duke Confidentiality Agreement. (this is a 1 time only request made when hired, but verify all existing and new staff have signed)

____ I will present my research in progress and findings annually to other investigators in a GIM forum that allows open and critical discussion of the data and its analysis.

____ I am aware of the GIM Division Integrity Coordinator and Integrity Officer, to whom any concern or question about research data management can be taken by any individual inside or outside the division.

____ I have been informed about the various school, department and division resources that support researchers and their activities.

____ I have reinforced that my highest priority is to obtain the true result of all studies, irrespective of the effect such a result may have on the overall project, grant submission, or manuscript.

____ I have a zero-tolerance policy with respect to data manipulation, alteration, or falsification and all of my research staff are aware of the consequences for data manipulation, alteration, or falsification (immediate termination).

____ I will observe my research staff during the data collection process and will periodically spot-check the data.

____ I have engaged (current projects) and/or will engage (future projects) appropriate collaborators, statisticians, and other relevant team members for constructive input before actual research studies begin.

____ I will develop well-defined study goals for my research studies.

____ I have or will implement a policy of best practices with respect to research records, including use of standard data collection and entry procedures, minimal use of paper data collection, and data storage in standard, secure databases such as REDCap.

____ I have or will leverage institutional resources such as the Duke Biobank, REDCap, Pedigene or other similar centralized infrastructure that limits users, directly obtains input from source elements, and tracks all changes in the data elements or samples.

____ I have (current studies) and/or will implement (future studies) a procedure to permanently archive raw data in a secure location that can only be accessed by the PI or a specified delegate.

____ I have developed a plan with my collaborators to ensure data provenance and integrity.

____ I have a plan to independently replicate study results.

____ I, or a designate, will re-analyze all critical studies, such as those included in grant or manuscript submissions, starting with the archived raw data.

____ I have developed a process (e.g. team meeting notes or PI notes) to document critical results, the date I learned of them, the interpretation of these results, and conclusions or discoveries that these results imply, as well as any procedures taken to confirm the validity of these results.

____ I confirm that I feel comfortable voicing any and all concerns about the integrity of someone's data, be it my research or someone else's.

____ I have a mechanism in place within my research team to prevent misconduct and handle research-related complaints.

Faculty Member Printed Name: _____

Faculty Member Signature: _____ Date: _____

## Science Culture and Accountability Plan

## GIM Checklist for Research Staff

The **Duke Division of General Internal Medicine** (GIM) is committed to maintaining the highest quality and integrity of all its research data. GIM is committed to ensuring that policies and procedures are in place to reflect the highest professional conduct and to promote a culture in which scientific results are critically reviewed and accountability for data integrity is clearly delineated.

Each member of the Division of General Internal Medicine (faculty, staff, administrators, fellows, students, trainees, volunteers, students, post-docs, or anyone who is or will be involved in IRB protocols) is expected to reflect and pursue these values.

These documents have been developed to ensure the proper and secure handling of human subject research-related data, as well as administrative information related to research conducted in GIM. The purpose is to ensure that all data security measures, responsibilities and best practices are clearly delineated for GIM members.

All GIM personnel who are or will be involved in IRB protocols are required to review and complete these document prior to handling any research data within GIM.

**Indicate with a Y for Yes or N for No for each item.**

____ I have reviewed this SOP document.

____ I have completed all required institutional training modules related to responsible data management and have taken advantage of programs offered through the SOM that are designed to address research integrity.

____ I have completed the Data Integrity and Security class presented by DOCR. (this is a 1 time only class)

____ I have signed the required Duke Confidentiality Agreement. (this is a 1 time only request made when hired)

____ I am aware of the GIM Division Integrity Officer, to whom any concern or question about research data management can be taken by any individual inside or outside the division.

____ I have been informed about the various school, department and division resources that support researchers and their activities.

____ I have reinforced that my highest priority is to obtain the true result of all studies, irrespective of the effect such a result may have on the overall project, grant submission, or manuscript.

____ I understand that the department, division as well as my PI(s) has a zero-tolerance policy with respect to data manipulation, alteration, or falsification and I am aware of the consequences for data manipulation, alteration, or falsification (immediate termination).

____ I understand I will be observed during the data collection process.

____ I will follow policies of best practices with respect to research records, including use of standard data collection and entry procedures, minimal use of paper data collection, and data storage in standard, secure databases such as REDCap.

____ I confirm that I feel comfortable voicing any and all concerns about the integrity of someone's data, be it my PIs research or someone else's.

____ I will follow the mechanisms in place within my research team to prevent misconduct and handle research-related complaints.

Research Staff Member Printed Name: _____

Research Staff Member Signature: _____ Date: _____

# APPENDIX 2

# Duke Division of General Internal Medicine Science Culture and Accountability Plan Faculty Checklist for Research Projects

## Science Culture and Accountability Plan

## GIM Faculty Checklist for Research Projects

## Recommended practices for improving the culture of scientific accountability within your individual research project

The principles above provide guidance for ensuring the integrity of your own data and for maintaining compliance with the DOM SCAP. You should discuss these expectations with your research team, and develop explicit processes within your project to monitor compliance with these policies. It is expected that you will review the steps you have taken to comply with this policy at your annual review meeting with your division chief.

- As a principle investigator, you set the example for your team through honest and open discussion of results and through your emphasis on scientific integrity and data quality over positive results. Do not, in any way, encourage or put pressure on lab personnel to obtain specific results. Make it clear at all times that your highest priority is to obtain the true result of all studies, irrespective of the effect such a result may have on the overall project, grant submission, or manuscript. Make it clear that you have a zero-tolerance policy with respect to data manipulation, alteration, or falsification.
- High-quality research begins with careful planning and study design. Engage appropriate collaborators, statisticians, and other relevant team members for constructive input before actual experiments or clinical studies begin. Having well-defined study goals protects against fraud and improves the quality of results. Frame your research questions in ways that allow negative and positive results to be interesting and useful to your lines of inquiry; that is, refrain from expectations that one type of result is more valuable than another. Plan for multiple methods, techniques or analytic approaches for reproducing and comparing results from your experiments.
- Most of us rely on our trust of and judgment in others to ensure the integrity of our data. However, this alone is not sufficient. Examples exist where even the most seemingly trustworthy people have manipulated data. While you should continue to put your faith in others, you should reinforce this with specific practices and institute processes to ensure that your data is managed responsibly. Cross-train project personnel so that one person can independently verify the results of another, and so that no one person is alone in providing data or analysis.
- Implement a policy of best practices with respect to research records, including basic project notebooks/reports or clinical research records. When possible, utilize electronic recording solutions that automatically record date and timestamps of entries and data changes. Ensure that entries are being made in a way that conforms to policy. Make this policy clear to all project staff and enforce it. We recommend you review project notebooks/reports any time you meet to discuss data. Additionally, consider performing periodic audits of project notebooks/reports to ensure that a third-party reviewer would be satisfied with the level of documentation provided. With regards to clinical research, maintain all appropriate documents in accordance with all regulatory and IRB requirements. Consider the implementation of competency training specific to individual project or clinical research tasks.
- Rather than create your own individual clinical research or project database, leverage institutional resources such as the Duke Biobank, REDCap databases, Pedigene or other similar centralized infrastructure that limits users, directly obtains input from source elements, and tracks all changes in the data elements or samples.

- For any generated data, implement a procedure by which the data is permanently archived in a secure location that can only be accessed by you or a specific delegate. This may include digital data transferred to a secure server, data burned to CDs, or hard copy printouts archived in a place other than individual lab notebooks. Ideally, this data would be stored in a read-only format that could not be altered once it is deposited. Most divisions within the Department of Medicine have server space available for investigators. The U.S. Department of Health and Human Services requires that all project data be retained for at least 3 years after the funding period ends.
- Develop a plan with collaborators to ensure data integrity. For example, you may request a copy of the raw data generated by your collaborators for archiving on your own. Similar to data analysis performed for your project-generated data, when possible, perform an independent analysis of data generated by collaborators to verify accuracy.
- You or a designate should re-analyze all critical studies, such as those included in grant or manuscript submissions, starting with the archived raw data. You may consider including a person with the appropriate expertise outside your team. For clinical or translational studies, this can be accomplished by having study results independently analyzed by a statistician separate from the investigative team.
- Develop a process (e.g. PI notebook) in which you document critical results, the date you learned of them, your interpretation of these results, and conclusions or discoveries that these results imply. In addition, you should document procedures you have taken to confirm the validity of these results, such as your own review of the raw data and your re-analysis and conclusions. These records will allow you to document the intellectual progress of specific projects to develop future hypotheses or research plans, and if needed, to support intellectual property claims. Furthermore, if questions of data integrity were to arise, such a notebook would serve to document that you verified all critical studies to the full extent possible.
- All individuals engaged in research will be required to complete online training modules, similar to those required by IACUC and the IRB, that emphasize these principles. (The Department and SOM will collaborate to develop these new modules). In addition, individuals should also take advantage of programs offered through the SOM that are designed to address research integrity. Additional competency training for investigators and their research staff can include the current core curriculum from Duke Office of Clinical Research, i.e. Informed Consent Process, Study Documentation, Data Integrity and Security, and annual Human Subject Research Overview for clinical investigators. At a faculty level, participation in institutional programs such as LEADER will provide opportunity for further education in research management and oversight.
- If you have concerns about the integrity of someone's data, be it in your project or someone else's, you should feel comfortable voicing your concerns. This is true whether you think a certain analytic method needs to be better validated or if you suspect scientific misconduct.
- Raising concerns about data integrity is not the same thing as accusing someone of scientific misconduct. The Department of Medicine wishes to promote a culture in which all aspects of scientific findings are critically reviewed. This includes all steps in the scientific process, from study design to data acquisition to methods of analysis to the formulation of conclusions. Raising and responding to questions about data integrity should be a routine part of the critical review process – in other words, it need not be reserved solely for cases of suspected scientific misconduct. It is through this process that we all can work together to ensure the highest possible quality of science at Duke.
- Have a mechanism in place within your project or research team to prevent misconduct and handle research-related complaints, reflecting a no-tolerance policy related to falsifying data, deceptive advertising, or enrollment of subjects not qualified to be in studies.
- If your project engages in translational or genomics research, plan biannual discussions with your staff about the challenges inherent to that research. Review the existing and new resources available across Duke, especially those to make your research more reliable and transparent.

Please confirm the following:

| | |
|---|---|
| PI Initials _____ | I have reviewed and will abide by the policies addressed in the latest “Operating Procedures for Science Culture and Accountability and Data Integrity and Security” manual for this research project. |
| PI Initials _____ | I confirm that my research team(s) has reviewed the latest “Operating Procedures for Science Culture and Accountability and Data Integrity and Security” manual and have promised to abide by the policies. |
| PI Initials _____ | I have discussed these expectations with my research team(s) and have developed explicit processes within my project to monitor compliance with these policies for this research project. |
| PI Initials _____ | I confirm that I, and my research team, are abiding by all Duke and GIM policies. |

PI Printed Name: _____

PI Signature: _____ Date: _____

# APPENDIX 3

# Duke Department of Medicine
# Science Culture and Accountability Plan

**Duke** Department of Medicine
Duke University School of Medicine

# Science Culture & Accountability Plan

Duke University is committed to maintaining the highest quality and integrity of all its scientific enterprise. Because of this commitment, the School of Medicine (SOM) is required to have mechanisms to guarantee the responsible management and critical review of scientific data. This is analogous to the School's obligation to ensure lab safety, proper clinical study procedures, and the appropriate use of animals in research.

The School of Medicine has created the Advancing Scientific Integrity, Services and Training (ASIST) office to support individual departments in adopting and implementing policies and procedures related to best practices for scientific accountability and integrity. The Department of Medicine (DOM) is committed to ensuring that departmental policies and procedures are in place to maintain the highest level of professional conduct – to promote a culture in which scientific results are critically reviewed, accountability for data integrity is clearly delineated, concerns can be to be brought forth without hesitation, and that there are mechanisms by which these concerns can be addressed fairly and expeditiously.

In the Department of Medicine, we recognize this requires appropriate aptitude and active participation of all parties in the research mission, from trainees to the department chair. In recent years, events at Duke and elsewhere have highlighted the ongoing need for explicit processes and mechanisms to manage scientific research data in a responsible manner. At the same time, most investigators have received little, if any, training or guidance in this area. Therefore, the DOM will ensure that all relevant faculty engaged in research document competency in responsible conduct of research or complete training through in person or web based modules as required by the Duke SOM ASIST office.

**Principles**
The Department of Medicine has prepared the following Science Culture & Accountability Plan (DOM-SCAP). This plan details three levels of responsibility – individual, division and department – for promoting a culture that encourages responsible data management and produces data of the highest integrity. The DOM-SCAP reflects these important principles:

1. We foster an environment where scientific integrity is the highest priority.
2. We emphasize high-quality, reproducible data and results.
3. We value constructive critiques of research.
4. We encourage open discussion of any concerns regarding research conduct or integrity.

Each and every member of the Department of Medicine – faculty, trainees, staff and administrators – is expected to reflect and pursue these values. Ours is a shared commitment to the highest standards of scientific activity.

**Questions or comments**
Contact Scott Palmer, M.D., Vice Chair for Research, at scott.palmer@dm.duke.edu or Erica Malkasian, M.B.A., Director Research Administration at erica.malkasian@duke.edu.

*Last updated January 4th 2018*

**1. Recommended practices for improving the culture of scientific accountability within your individual laboratory**

The principles above provide guidance for ensuring the integrity of your own data and for maintaining compliance with the DOM-SCAP. You should discuss these expectations with your research team, and develop explicit processes within your lab to monitor compliance with these policies.

It is expected that you will review the steps you have taken to comply with this policy at your annual review meeting with your division chief.

- As a principal investigator, you set the example for your team through honest and open discussion of results and through your emphasis on scientific integrity and data quality over positive results. Do not, in any way, encourage or put pressure on lab personnel to obtain specific results. Make it clear at all times that your highest priority is to obtain the true result of all studies, irrespective of the effect such a result may have on the overall project, grant submission, or manuscript. Make it clear that you have a zero-tolerance policy with respect to data manipulation, alteration, or falsification.
- High-quality research begins with careful planning and study design. Engage appropriate collaborators, statisticians, and other relevant team members for constructive input before actual experiments or clinical studies begin. Having well-defined study goals protects against fraud and improves the quality of results. Frame your research questions in ways that allow negative and positive results to be interesting and useful to your lines of inquiry; that is, refrain from expectations that one type of result is more valuable than another. Plan for multiple methods, techniques or analytic approaches for reproducing and comparing results from your experiments.
- Most of us rely on our trust of and judgment in others to ensure the integrity of our data. However, this alone is not sufficient. Examples exist where even the most seemingly trustworthy people have manipulated data. While you should continue to put your faith in others, you should reinforce this with specific practices and institute processes to ensure that your data is managed responsibly. Cross train lab personnel so that one person can independently verify the results of another, and so that no one person is alone in providing data or analysis.
- Implement a policy of best practices with respect to research records, including basic laboratory notebooks or clinical research records. When possible, utilize electronic recording solutions that automatically record date and timestamps of entries and data changes. Ensure that entries are being made in a way that conforms to lab policy. Make this policy clear to all lab personnel and enforce it. We recommend you review people's lab notebooks any time you meet with them to discuss data. Additionally, consider performing periodic audits of laboratory notebooks to ensure that a third-party reviewer would be satisfied with the level of documentation provided for an experiment. With regards to clinical research, maintain all appropriate documents in accordance with all regulatory and IRB requirements. Consider the implementation of competency training specific to individual lab or clinical research tasks.
- Rather than create your own individual clinical research or laboratory database, leverage institutional resources such as the Duke Biobank, REDCap databases, Pedigene or other

similar centralized infrastructure that limits users, directly obtains input from source elements, and tracks all changes in the data elements or samples.

- For any data that is generated by instruments, such as plate readers, scintillation counters, cameras, flow cytometers, etc., require personnel to include the specific instrument, its location, and the date and time the analysis was performed in their lab notebook. This will make it easier to match the lab notebook with instrument-generated raw data. In addition, maintain frequent monitoring, calibration, and validation of all laboratory equipment.
- For any instrument-generated data, implement a procedure by which the raw instrument-generated data is permanently archived in a secure location that can only be accessed by you or a specific delegate. This may include digital data transferred to a secure server, data burned to CDs, or hard copy printouts archived in a place other than individual lab notebooks. Ideally, this data would be stored in a read-only format that could not be altered once it is deposited. Most divisions within the Department of Medicine have server space available for investigators. The U.S. Department of Heath and Human Services requires that all project data be retained for at least 3 years after the funding period ends.
- Develop a plan with collaborators to ensure data integrity. For example, you may request a copy of the raw data generated by your collaborators for archiving in your own lab. Similar to data analysis performed for your laboratory-generated data, when possible, perform an independent analysis of data generated by collaborators to verify accuracy.
- To the extent possible, independently replicate study results. For example, have different people perform experimental procedures (such as treating groups of mice with a drug) and experimental readouts (such as determining the phenotype of the treated mice). It is also good practice to require that persons assaying readouts be blinded to the experimental groups.
- You or your designee should re-analyze all critical studies, such as those included in grant or manuscript submissions, starting with the archived raw data. You may consider including a person with the appropriate expertise outside your lab. For clinical or translational studies, this can be accomplished by having study results independently analyzed by a statistician separate from the investigative team.
- Develop a process (e.g. PI notebook) in which you document critical results, the date you learned of them, your interpretation of these results, and conclusions or discoveries that these results imply. In addition, you should document procedures you have taken to confirm the validity of these results, such as your own review of the raw data and your re-analysis and conclusions. These records will allow you to document the intellectual progress of specific projects to develop future hypotheses or research plans, and if needed, to support intellectual property claims. Furthermore, if questions of data integrity were to arise, such a notebook would serve to document that you verified all critical studies to the full extent possible.
- All individuals engaged in research will be required to complete online training modules, similar to those required by IACUC and the IRB, that emphasize these principles. Individuals should also take advantage of programs offered through the SOM that are designed to address research integrity. Additional competency training for investigators and their research staff can include the current core curriculum from Duke Office of Clinical Research, i.e. Informed Consent Process, Study Documentation, Data Integrity and Security,

and annual Human Subject Research Overview for clinical investigators. At a faculty level, participation in institutional programs such as LEADER will provide opportunity for further education in research management and oversight.

- If you have concerns about the integrity of someone's data, be it in your lab or someone else's, you should feel comfortable voicing your concerns. This is true whether you think a certain analytic method needs to be better validated or if you suspect scientific misconduct.
- Raising concerns about data integrity is not the same thing as accusing someone of scientific misconduct. The Department of Medicine wishes to promote a culture in which all aspects of scientific findings are critically reviewed. This includes all steps in the scientific process, from study design to data acquisition to methods of analysis to the formulation of conclusions. Raising and responding to questions about data integrity should be a routine part of the critical review process – in other words, it need not be reserved solely for cases of suspected scientific misconduct. It is through this process that we all can work together to ensure the highest possible quality of science at Duke.
- Have a mechanism in place within your laboratory or research team to prevent misconduct and handle research-related complaints, reflecting a no-tolerance policy related to falsifying data, deceptive advertising, or enrollment of subjects not qualified to be in studies.
- If your lab engages in translational or 'omics research, plan biannual discussions with your staff about the challenges inherent to that research. Review the existing and new resources available across Duke, especially those to make your research more reliable and transparent.

**2. Recommended safeguards to ensure data integrity within your division**

The Department of Medicine believes that the proper accountable unit for ensuring data integrity is the division. For this reason, all divisions within the Department of Medicine should follow the key principles and steps outlined in this Science Culture & Accountability Plan. Although this document outlines the best practices with regards to scientific accountability, we also recognize that within each division not all steps, or the same set of activities, may be appropriate. In addition, divisions may establish multiple accountable units to better interface with specific groups of investigators. Ultimately, the Department requires that the division chiefs maintain evidence of compliance with the DOM-SCAP on behalf of their divisions, as suggested below.

- Divisions must ensure that all divisional investigators and personnel engaged in scientific research complete all required institutional training modules in responsible data management. These will be developed and monitored for compliance through central SOM resources, similar to the IRB modules required for studies involving human subjects.
- Divisions must ensure that all divisional investigators implement and maintain policies for responsible data management within their labs or research groups. Divisions must also establish mechanisms by which the validity and integrity of critical data generated by every division investigator can be confirmed. These mechanisms should not place an undue burden on the investigators or the division but should ensure that investigators are adhering to policies of responsible data management. These policies should be reviewed at

least once a year by the division chief, an appropriate representative of the division chief, or the individual directing the accountable research unit. For example you may specifically review and assess compliance at an individual level with all the points in Step 1 as part of a yearly meeting with each faculty member in your division.

- Divisions must ensure that all investigators regularly present their research findings to other investigators outside their own lab or research group in a forum that allows open and critical discussion of the data and its analysis. Examples include participation in other lab meetings, regularly schedule multi-disciplinary group meetings thematically organized around common research interests, or a divisional work-in-progress series. In order to monitor compliance, we suggest maintaining log sheets of faculty participation in these conferences.
- Review and follow best practices for data integrity and manuscript preparation as required by the top journals in your field(s).
- Divisions must identify a Division Integrity Coordinator, to whom any concern or question about research data management can be taken by any individual inside our outside the division. This contact person may be the division chief or one or more designees.
- Division leaders are expected to confirm that each investigator is aware of the various school, department and division resources that support researchers and their activities, including access to statistician input and review of study design, analysis and publication.
- Divisions are encouraged to require that faculty and staff complete the Data Integrity and Security class presented by DOCR, as appropriate.
- Explore ways for lab personnel to report to more than one investigator.

**3. Departmental efforts to promote a culture of scientific accountability.**

The Department of Medicine leadership will also take steps to support, guide and ensure a culture of scientific integrity, including the actions listed below.

- Outline a chain of persons available to address research integrity concerns. These division integrity coordinators will be available to assist faculty and staff within the divisions. Concerns can also be raised to a division chief, but in case of real or perceived conflict of interest, concerns may be raised to a departmental vice chairs or to the chair.
- Work with the SOM to develop institutional policies and modules in training of responsible conduct of research and ensuring data integrity.
- Work with all the Centers or Institutes in which faculty from the DOM reside to ensure alignment and integration with their programs of scientific accountability. Faculty that participate in DOM and Duke Centers or Institute are expected to comply with SCAP principles as outlined by both DOM and Center or Institute but would only need to complete required ASIST training once.
- Leverage the existing Medicine Research Conference to focus on case studies of scientific misconduct to better educate the Department about processes to prevent fraud, highlight opportunities to improve the research culture, and establish best practices in the laboratory with regards to research integrity.

*January 2018*

- Develop an on boarding program for new investigators that includes an emphasis on the principles outlined above. Strengthen the understanding that adhering to the SCAP principles is relevant to how we provide patient care and useful to future studies in humans.
- Require each investigator with active IRB protocol(s) to complete role-based training in Informed Consent Process, Data Integrity and Security and Study Documentation, as coordinated by the Medicine Clinical Research Unit.
- Promote the sharing of best practices regarding data integrity through partnership with ASIST office
- Educate the faculty and staff of the Department about available resources and reporting mechanisms for scientific accountability, such as:
  - The NIH Office of Research Integrity (http://ori.dhhs.gov/)
  - Guidelines for the Proper Handling of Digital Image Data (http://jcb.rupress.org/content/166/1/11.full)
  - Online Learning Tool for Research Integrity and Image Processing (http://ori.hhs.gov/education/products/RIandImages/default.html)
  - The Compliance and Fraud Hotline: To anonymously report a suspected compliance violation or concern, the Compliance and Fraud Hotline at Duke is at 800-849-9793.

# APPENDIX 4

# Additional References and Links

Acceptable Use Policy: http://security.duke.edu/duke-acceptable-use-policy

Account or Data Access Policy: https://security.duke.edu/policies/account-or-data-access-policy

Compliance and Fraud Hotline at Duke: 800-849-9793 (anonymously report a suspected compliance violation or concern)

Duke Confidentiality Agreement: https://hr.duke.edu/forms/confidentiality-agreement

Copyright/DMCA: https://security.duke.edu/copyrightdmca

Duke Corrective Action Policy:
http://www.hr.duke.edu/policies/expectations/standards/corrective_action.php

Duke Data Classification Standard: https://security.duke.edu/policies/data-classification-standard

Duke Faculty Handbook: http://www.provost.duke.edu/policies/fhb.html

Duke Health Mobile Device Manager: https://mobile.dhts.duke.edu/message-duke-health-leadership

Duke Incident Management Procedures: https://security.duke.edu/services/incident-management

Duke HR Payroll Data Policy: https://forms.hr.duke.edu/forms/hrdata/policy.php

Duke Office of Clinical Research (DOCR) – Planning for Data Collection and Monitoring:
https://medschool.duke.edu/research/clinical-and-translational-research/duke-office-clinical-research/irb-and-institutional-10

Duke Office of Research Support - Policies for the Responsible Conduct of Research:
https://ors.duke.edu/orsmanual/policies-responsible-conduct-research

Duke Policy on Social Security Number Usage: https://security.duke.edu/policies/social-security-number-usage-policy

Duke Staff Handbook: https://hr.duke.edu/policies

Duke Vendor Risk Assessment: https://security.duke.edu/vendor-risk-assessment

Duke Vulnerability Management Policy: https://security.duke.edu/policies/vulnerability-management

FERPA: https://registrar.duke.edu/student-records

FISMA: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

Guidelines for the Proper Handling of Digital Image Data: http://jcb.rupress.org/content/166/1/11.full

HIPAA: http://www.hhs.gov/ocr/privacy/

Human Resources Policies: https://www.hr.duke.edu/policies/

National Institutes of Health HIPAA Privacy Rule Information for Researchers:
https://privacyruleandresearch.nih.gov/pr_08.asp

NC Identity Theft Protection Act: http://www.ncga.state.nc.us/sessions/2005/bills/senate/html/s1048v6.html

Online Learning Tool for Research Integrity and Image Processing:
http://ori.hhs.gov/education/products/RIandImages/defulat.html

PCI-DSS - Guidelines for Responsible Data Management in Scientific Research:
https://ori.hhs.gov/images/ddblock/data.pdf

The NIH Office of Research Integrity: https://ori.hhs.gov