ADVOCATE HEALTH	
Title: Research Security Policy (Enterprise)	**Published Date:** 10/30/2025 **Last Review / Revised Date:** 10/30/2025
Document Type: ☒ Policy ☐ Procedure ☐ Guideline ☐ Other	**Content Applies to Patient Care:** ☐ Adults ☐ Pediatrics (Under 18) ☒ N/A
Scope: ☒ Enterprise ☐ Division(s): ☐ Area Name: ☐ Entity Name: ☐ Department Name:	

I. PURPOSE

The purpose of this policy is to safeguard Advocate Health's research endeavors against threats to national and economic security, ensuring the integrity and ethical conduct of research while fostering an open and collaborative research environment.

II. SCOPE

This policy applies to all individuals conducting research under the auspices of Advocate Health, and its respective affiliates, regardless of the funding source or location.

III. DEFINITIONS / ABBREVIATIONS

Covered Individual: An individual who contributes significantly to a research and development project funded by a federal agency or is designated as a covered individual by that agency. Covered Individuals generally includes senior and key personnel, such as Principal Investigators and Co-PIs, as well as others who substantially contribute to the project's scientific progress. federal agencies have the discretion to define who they considered a 'Covered Individual'.

CUI: Controlled Unclassified Information.

DCP: Data Control Plan.

Data Control Plan: A formal management plan that outlines the specific procedures and safeguards implemented to protect CUI.

DPI: Digital Persistent Identifier.

Export: There are three ways an export may occur: (1) The actual shipment or transmission of items out of the U.S., including to U.S. citizens abroad. This encompasses physical goods, scientific equipment, and materials shipped via any method, including hand-carrying during travel; (2) The electronic or digital transmission of any covered items, technology, or related information leaving

U.S. borders. This includes transfers via email, cloud storage, or other digital means, and (3) The release or disclosure of export-controlled technology, software, or technical data to any foreign national regardless of their location.

Export-controlled information: Unclassified information whose transfer or disclosure, including to foreign nationals within the U.S., is restricted or controlled by U.S. laws and regulations for reasons of national security, foreign policy, anti-terrorism, or non-proliferation.

FCOC: Foreign Country of Concern.

Foreign Countries of Concern: North Korea, Iran, Russia, Belarus, China (including the Special Administrative Regions of Hong Kong and Macau), Cuba, Venezuela, or the Crimea, Donetsk, and Luhansk regions of Ukraine and any future countries as identified by the U.S. government.

FTRP: Foreign Talent Recruitment Program.

Foreign Talent Recruitment Programs: A program, position, or activity offering compensation from a foreign entity for an individual's knowledge and expertise. Compensation can include various forms like cash, funding, travel, honorific titles, or career advancement opportunities.

Insider Threat: The potential for an individual with authorized access to Advocate Health's resources to use such resources, either wittingly or unwittingly, to cause harm to the Research Enterprise or its stakeholders. This harm can include, but is not limited to espionage, theft of intellectual property, or research data, sabotage of systems or facilities, unauthorized disclosure of information, or workplace violence.

Malign Foreign Talent Recruitment Programs: A FTRP sponsored by a FCOC that includes problematic requirements. The focus on these programs has increased due to concerns about their potential use by foreign governments to acquire U.S. scientific research and valuable intellectual property, sometimes through illicit means (see the CHIPS and Science Act of 2022 for a more detailed definition of MFTRPs).

MFTRPs: Malign Foreign Talent Recruitment Programs.

NIH: National Institutes of Health.

NIST: National Institute of Standards and Technology.

NSPM-33: National Security Presidential Memorandum-33.

ORCID iD: Open Researcher and Contributor ID.

PI: Principal Investigator.

Research Enterprise: Advocate Health including all of its affiliates, regardless of their location.

Research Security: The principles and actions that protect the Research Enterprise from misappropriation, violations of research integrity, and foreign government interference. They are the collective system of controls that safeguards the Research Enterprise against threats to national and economic security integrity. This includes regulations, policies and procedures that protect the Research Enterprise from theft, misuse and unauthorized access. It also mitigates insider threats and foreign influence.

RISRA: Research Integrity, Security, and Regulatory Affairs Office.

IV. POLICY

National Security Presidential Memorandum-33 ("NSPM-33") is a U.S. government directive issued in January 2021 calling on federal research funding agencies to require a Research Security program at recipient organizations receiving more than $50 million annually in federal research funding. NSPM-33 also seeks consequences for non-disclosure of foreign affiliations and provides guidance for sharing information on violations across federal research funding agencies.

The White House Office of Science and Technology Policy further issued implementation guidance ('Guidelines for Research Security Programs at Covered Institutions') providing additional clarity on Research Security program requirements including details on training requirements, foreign travel security, and cybersecurity. Final guidelines were published on July 9, 2024, for agency implementation.

Research Security is centered around the following four key areas:

1. International travel;
2. Export control training;
3. Cybersecurity; and
4. Research security training.

By practicing Research Security, we safeguard information, data, technological advancement, and U.S. economic and national security. Every one of us chairs responsibility for maintaining security. Our collective efforts help the research community protect unpublished work intellectual property and reputation. Our commitment will retain our culture of innovation, trust, and collaboration and ensure good stewardship of sponsored funds.

V. INTERNATIONAL TRAVEL

International travel is often essential for conducting research, presenting findings, and fostering collaborations. However, it can also pose risks to Research Security, including the inadvertent or illicit transfer of sensitive information, technology, or intellectual property. Advocate Health is committed to ensuring that our researchers can travel safely and securely while adhering to all applicable regulations.

A. All international travel related to Advocate Health research activities, regardless of funding source, must be booked via Advocate Health's travel booking tool: Deem Travel.
B. Travel to Foreign Countries of Concern are subject to an automatic export control review processed by the Research Integrity, Security, and Regulatory Affairs Office ("RISRA").
C. Researchers traveling to Foreign Countries of Concern are encouraged to:
    a. take a clean/loaner laptop that does not contain any export-controlled technology, sensitive, or proprietary/confidential information. A clean laptop can be checked out at the following locations:
        i. Carpenter Library, School of Medicine (Main Campus), Academic Computing Lab, 3rd Floor and
        ii. BGCME Resource Center, 475 Vine St., Winston-Salem, NC 27101 (Downtown, Innovation Quarter)
    b. review the pre-travel brief information on the intranet.
D. Researchers traveling to international locations not designated as a Foreign Country of Concern are encouraged to:
    a. Minimize the amount of sensitive, proprietary, or unpublished data stored on electronic devices carried during travel.
    b. Back up all data and information before traveling and store the backup on a OneDrive maintained by Advocate Health.
    c. Consider using a clean/loaner laptop when available.
    d. review the pre-travel brief information on the intranet.

VI. EXPORT CONTROL TRAINING

Export control laws are federal laws that regulate the transfer of items, information, and software deemed sensitive for national security and foreign policy reasons. These laws apply to all international activities, regardless of funding source.

Regular training is a crucial element of Advocate Health's export control compliance program. It is designed to equip all members of Advocate Health with the knowledge necessary to comply with federal regulations and prevent costly violations.

By adhering to the training requirements below, Advocate Health aims to cultivate a robust culture of export control compliance, minimize risks, and safeguard its research activities.

A. Key personnel involved with research activities are required to take the Research Security training module, which includes export control training, once a year as part of their annual training requirements via Advocate Health's single cloud-based management system: Workday.
B. The RISRA Office will maintain records of completed training and a Researcher's training record may be monitored, particularly those involved in high-risk activities.
C. All personnel involved in research are also encouraged to voluntarily take the Research Security training module to help understand the basics of export controls, as activities in various departments can inadvertently lead to violations.
D. The Collaborative Institutional Training Initiative (CITI Program) offers a comprehensive suite of web-based modules on export controls that have been purchased by Advocate Health and are available to all personnel involved in research. This series is a set of modules for voluntary self-paced learning. The following modules are highly recommended:
    i. Introduction to Export Compliance
    ii. Export Compliance for Researchers
    iii. Export Compliance for Research Administrators
    iv. Export Compliance and Biosafety
    v. Export Compliance for International Shipping
E. For more information regarding export controls please see Advocate Health's Export Control Policy.

VII. CYBERSECURITY

Cybersecurity is a critical component of research security, protecting research data, systems, and intellectual property from unauthorized access, loss, or manipulation. Advocate Health is committed to implementing robust cybersecurity measures to safeguard its Research Enterprise and ensure the integrity and confidentiality of research data.

The following safeguarding protocols and procedures have been established to satisfy the requirements of federal agencies:

A. Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
B. Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
C. Verify and control/limit connections to and use of external information systems.
D. Control any non-public information posted or processed on publicly accessible information systems.
E. Identify information system users, processes acting on behalf of users, or devices.

F. Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
G. Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
H. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
I. Provide protection of scientific data from ransomware and other data integrity attack mechanisms.
J. Identify, report, and correct information and information system flaws in a timely manner.
K. Provide protection from malicious code at appropriate locations within organizational information systems.
L. Update malicious code protection mechanisms when new releases are available.
M. Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.
N. Provide regular cybersecurity awareness training for authorized users of information systems, including recognizing and responding to social engineering threats and cyber breaches.
O. All research involving Controlled Unclassified Information ("CUI") must be accessed via a system approved by Advocate Health Cybersecurity that meets the standards of NIST 800-171.
P. Use of any external storage systems, outside of approved networks, is strictly forbidden unless approved by the RISRA Office prior to such use.

These protocols and procedures are implemented via operational practice and policy via the: Access Control Policy, Anti-Virus Policy, Authorization and Acceptable Use Policy, Computer Equipment and Media Disposal and Reuse Policy, Data and System Integrity Policy, Data Governance Policy, Encryption Policy, FISMA General Policy, Incident Response Policy, Information Security Policy, Information System Activity Review Policy, ITS Risk Management Policy, Password Security Policy, Payment Card Security Policy, Privacy and Security Telecommuting Standards Policy, Privacy and Security Awareness Policy, Security Patching Policy, Server Security Policy, and the Workstation Security Policy.

VIII. INFORMATION OR DATA REQUIRING INCREASED SAFEGUARDING

Controlled Unclassified Information ("CUI")

CUI, established by Executive Order 13556, is information the U.S. Government creates or possesses, or that an entity creates or possesses for or on behalf of the U.S. government, which requires safeguarding, or dissemination controls

pursuant to and consistent with applicable law, regulations, and government-wide policies.

A. It is the responsibility of the researchers associated with projects involving CUI to notify the RISRA Office upon award of a project involving the creation, handling, or storage of CUI. Prior to beginning a project involving CUI, a Data Control Plan ("DCP") must be submitted and approved by the RISRA Office. A DCP must include the following information:
    a. Detailed procedures for protecting both paper and digital CUI (i.e. physical control, storage, etc.) to limit access to authorized users only;
    b. A list of all authorized users requiring access to CUI as part of the project;
    c. Media marking and distribution plan in accordance with applicable federal laws, executive orders, directives, policies, and regulations.
    d. If applicable, procedures for transporting CUI outside of controlled access areas;
    e. Procedures for sanitizing or destroying physical and/or digital CUI; and
    f. Other information may be required in the DCP, at the discretion of the RISRA Office.
B. The RISRA Office is responsible for screening individuals requiring access to CUI to ensure access is provided in accordance with federal regulations.
C. The researchers are responsible for notifying the RISRA Office if there are any changes to the approved list of authorized users (i.e., adding users to the project or termination/transfer of personnel no longer requiring access, etc.)

NIH Repository Data

NIH repository data refers to the vast collection of scientific and biomedical datasets stored and managed by the NIH. The NIH strongly encourages researchers to use established repositories to preserve and share scientific data, making it more findable, accessible, interoperable, and reusable.

The NIH supports and works with a wide range of repositories, from generalist options that accept all types of data to specialized repositories focused on specific scientific domains or data types.

A. Domain-specific repositories approved by the NIH may be found here: https://www.nlm.nih.gov/NIHbmic/domain_specific_repositories.html
B. Generalist repositories approved by the NIH may be found here: https://www.nlm.nih.gov/NIHbmic/generalist_repositories.html
C. Access to NIH repository data varies depending on the nature of the information:
    1. Open or unrestricted access: Datasets are available for public download without special credentials, though users are expected to use the data responsibly.

2. Registered access: Users must register with the repository to access the data, and their usage may be monitored.
3. Controlled access: For sensitive data, particularly involving human subjects, credentialed users must apply for access. This process ensures compliance with confidentiality and consent requirements.

D. All research involving NIH repository data must be accessed and stored via an NIH approved domain-specific or generalist repository.

E. Users accessing and storing data from an NIH Controlled-Access Data Repository (CADR) must store data in accordance with the "Required Security and Operational Standards for NIH Controlled-Access data Repositories" outlined in the NIH CADR Guidebook. Additionally, users accessing and storing data from a CADR designated as an NIH-Designated Genomic Data Repository must store data in accordance with the security standards outlined in the NIH Security Best Practices for Users of Controlled-Access Data.

F. Use of any external storage systems, outside of approved networks, is strictly forbidden unless approved by IT Technology Services prior to such use.

This data-sharing initiative serves key purposes such as advancing biomedical research, increasing transparency and reproducibility, and promoting collaboration.

U.S. Government-Related Data and/or Bulk Data Transfers

Contracts involving any U.S. government-related data or bulk U.S. sensitive personal data transfers to a Foreign Country of Concern are required to be reviewed from a privacy and research security perspective, as implemented by the National Security Division of the Department of Justice under Executive Order 14117.

Digital Persistent Identifiers ("DPI")

Researchers who are part of an application for, or who have received, federal funding are required to obtain a globally unique, persistent, machine resolvable and processable, digital ID possessing an associated metadata schema.

The central goal is to improve transparency and safeguard U.S. government-supported research and development from exploitation by foreign entities. By uniquely identifying researchers, DPIs help track disclosures of affiliations, funding, and potential conflicts of interest.

Researchers are required to provide their DPI in official forms, such as the Biographical Sketch and Current and Pending (Other) Support forms.

Advocate Health has adopted the Open Researcher and Contributor ID ("ORCID iD") as the official persistent identifier for all research personnel.

IX. MALIGNED FOREIGN TALENT RECRUITMENT PROGRAMS ("MFTRPs")

Advocate Health is committed to protecting the integrity of its Research Enterprise and complying with all U.S. laws and regulations concerning foreign influence in research, including those related to Foreign Talent Recruitment Programs ("FTRP") and expressly prohibits participation in MFTRPs to align with federal mandates.

The term "Maligned Foreign Talent Recruitment Program" is defined in the CHIPS and Science Act of 2022 (Sec. 10638) as:

Any program, position or activity compensated with cash or in-kind compensation such as complimentary foreign travel, honorific titles, career advancement opportunities, where the compensation is in exchange for one or more of the following:

1. Unauthorized transfer of intellectual property, materials, data products, or other nonpublic information developed through U.S. federal funding to a foreign government or entity affiliated with a foreign country;
2. Being required to recruit trainees or researchers to participate in the program or activity;
3. Establishing a lab or company or accepting a faculty position or other employment if these activities are in violation of standard terms and conditions of a federal award;
4. Being unable to terminate the contract except in extraordinary circumstances;
5. Requiring commitments that limit the capacity to carry out a U.S. federal award or would result in substantial overlap or duplication;
6. Being required to apply for or successfully receive funding from the sponsoring foreign government's funding agencies, with the foreign organization as the recipient;
7. Being required to omit acknowledgement of the recipient institution (i.e., Columbia University), or the U.S. federal research agency sponsor, contrary to institutional policies or standard award terms and conditions;
8. Being required to withhold information about participation in the program and not to disclose it to the U.S. funding agency or to Columbia; OR
9. Having a conflict of interest or conflict of commitment contrary to the standard terms and conditions of the award.

and

1. A foreign country of concern (FCOC) or an entity based in a FCOC, whether or not directly sponsored by the FCOC;
2. An academic institution on the list developed under section 1286(c)(8) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (NDAA 2019) (10 U.S.C. 2358 note; Public Law 115-232); or
3. A foreign talent recruitment program on the list developed under section 1286(c)(9) of the NDAA 2019 (10 U.S.C. 2358 note; Public Law 115-232).

Covered Individuals must disclose participation in any FTRP through Advocate Health's annual disclosure requirement process.

Researchers with federal funding must disclose FTRP participation to sponsors through required forms (e.g., Biographical Sketch, Current and Pending/Other Support).

If you have been approached by an organization that may meet the above definition, please contact the RISRA Office at mohammad.mahi@advocatehealth.org

X. RESEARCH SECURITY TRAINING

Regular training is a crucial element of Advocate Health's Research Security compliance program. It is designed to equip all members of Advocate Health with the knowledge necessary to comply with federal regulations and prevent costly violations.

By adhering to the training requirements below, Advocate Health aims to cultivate a robust culture of Research Security compliance, minimize risks, and safeguard its research activities.

A. Key personnel involved with research activities are required to take the Research Security training module once a year as part of their annual training requirements via Advocate Health's single cloud-based management system: Workday.
B. The Research Security training module covers:
    a. International travel;
    b. Export control training;
    c. Cybersecurity;
    d. Disclosure requirements;
    e. Insider threat awareness and identification;
    f. Risk Mitigation and Management;
    g. Importance of collaboration;
    h. U.S. policies and regulations;
    i. Reporting security incidents; and
    j. Proper handling and storage of CUI.

C. The RISRA Office will maintain records of completed training and a Researcher's training record may be monitored, particularly those involved in high-risk activities.
D. All personnel involved in research are also encouraged to voluntarily take the Research Security training module to help understand the basics of Research Security, as activities in various departments can inadvertently lead to violations.
E. Disclosure Requirement: Key Personnel involved with federal funding are required to disclose all research activities and affiliations (active and pending) within their Current and Pending/Other Support form as directed within NOT-OD-25-133.
    a. Key Personnel understand their responsibility to disclose all resources made available to the researcher in support of and/or related to all of their research endeavors, regardless of whether or not they have monetary value and regardless of whether they are based at the institution the researcher identifies for the current grant.

XI. RESEARCH SECURITY PROGRAM POINT OF CONTACT ("POC")

The below individuals are the designated Research Security POCs for the Research Enterprise:

- Derick R. Burgin
  Director, Research Integrity, Security, and Regulatory Affairs
  Derick.Burgin@advocatehealth.org

- M. Asif Mahi
  Manager, Export Controls and International Research Collaboration
  Mohammad.Mahi@advocatehealth.org

XII. CROSS REFERENCES

Travel & Business Expense Policy (NC/GA Division).
Travel & Business Expense Policy (IL & WI Divisions).
Export Control Policy.
Conflict of Interest – Research (Enterprise) Policy.

XIII. RESOURCES AND REFERENCES

United States Government. Presidential Memorandum on United States Government-Supported Research and Development National Security Policy. 2021. https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/

United States Government. Guidelines for Research Security Programs at Covered Institutions. 2024. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/OSTP-RSP-Guidelines-Memo.pdf

United States Government. Executive Order 13556—Controlled Unclassified Information. 2010. https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information

United States Government. CHIPS and Science Act (2022). https://www.congress.gov/bill/117th-congress/house-bill/4346

NIH Announces a New Policy Requirement to Train Senior/Key Personnel on Other Support Disclosure Requirements. https://grants.nih.gov/grants/guide/notice-files/NOT-OD-25-133.html

XIV. ATTACHMENTS

Not Applicable.

XV. REVISION DATES: 11/2022; 08/2024; 10/2025