

Research Integrity & Undue Foreign Influence

Why Foreign Influence Matters

As tensions between the U.S. and various foreign governments increase, accusations of academic espionage by foreign-supported researchers at U.S.-based research institutions are on the rise. The NIH, NSF, DOE, and other agencies are increasingly warning institutions of researchers who have not disclosed foreign associations in compliance with grant funding regulations and other laws. The government continues to initiate enforcement actions and we expect this to increase in frequency and scope during the coming months.

As a result, research and academic institutions in the U.S. need to be ever more vigilant to mitigate brand risk, the loss of federal funds, intellectual property assets and exposure to enforcement actions.

Securing Digital Materials

Amid concerns that individuals may be trying to steal research or replicate labs and systems, institutions should examine the steps they are taking to detect and prevent theft of digital research materials:

Issue	Available Tactics/Strategies to Mitigate Risk
Email	<ul style="list-style-type: none"> Require all personnel to use their official institutional email for research Prohibit the use of personal email for official business Consider auditing email use for evidence of off-system use for research (e.g., outliers in terms of volume of emails, identifying use of external emails among institutional colleagues)
Devices	<ul style="list-style-type: none"> Mandate use of institutional computers/devices/servers for research Require researchers to register personal devices with your IT department Deploy mobile device management tools to monitor personal devices and activate remote wipe capability
Storage	<ul style="list-style-type: none"> Require researchers to save materials – even drafts – to institutional shared drives or document-management systems to avoid loss of material and to create audit trails for access Discuss with your IT department whether they have capabilities to detect, monitor, log, and disable use of removable storage media (e.g., thumb drives) Consider prohibiting use of removable storage media in certain areas Require personnel to instead use secure file transfer services that offer encryption, password protection, expiration dates, identity verification, etc. Consider developing and permitting access for research materials only to institutionally-sanctioned cloud storage / sharing platforms
Policies / training	<ul style="list-style-type: none"> Review / revise policies related to acceptable use of institutional network and resources Confirm data security training is broad enough to address research integrity matters
Network	<ul style="list-style-type: none"> Consider network segmentation of departments with high-risk research / substantial federal grants
Audit	<ul style="list-style-type: none"> Monitor bulk transfers / downloads of data or other “unusual” network activity Network activity audit protocols may exist within HIPAA covered entity operations but may not exist or be enforced elsewhere in the organization (e.g., at academic medical centers)