NIH IT General Rules of Behavior

These Rules hold users accountable for their actions and responsible for information security. They apply to local, network, and remote use of HHS/NIH information (in both electronic and physical forms) and information systems by all NIH users, including federal employees, contractors, and other system users.

I assert my understanding that:

- Information and system use must comply with HHS and NIH policies and standards, and with applicable laws.
- Use for other than official, assigned duties is subject to the HHS Policy for Personal Use of Information Technology Resources.
- Unauthorized access to information or information systems is prohibited.
- Users must prevent unauthorized disclosure or modification of sensitive information, including Personally Identifiable Information (PII).

I must:

General Security Practices

- Follow NIH security practices whether working at my primary workplace or remotely;
- Accept that I will be held accountable for my actions while accessing and using HHS/NIH information and information systems;
- Ensure that I have appropriate authorization to install and use software, including downloaded software on NIH systems and that before doing so I will ensure that all such software is properly licensed, approved, and free of malicious code;
- Wear an identification badge (or badges, if applicable) at all times, except when they are being used for system access in federal facilities;
- Lock workstations and remove Personal Identity Verification (PIV) cards from systems when leaving them unattended;
- Use assigned unique identification and authentication mechanisms, including PIV cards, to access HHS/NIH systems and facilities;

- Complete the NIH Information Security and Information Management Trainings for New Hires before accessing any HHS/NIH system and on an annual basis thereafter, complete the NIH Information Security and Management Refresher and any specialized role-based security trainings, as required by HHS/NIH policies.
- Permit only authorized HHS/NIH users to use HHS/NIH equipment and/or software;
- Take all necessary precautions to protect HHS/NIH information assets (including but not limited to hardware, software, personally identifiable information (PII), protected health information (PHI), and federal records [media neutral]) from unauthorized access, use, modification, destruction, theft, disclosure, loss, damage, or abuse, and treat such assets in accordance with any information handling policies;
- **Immediately report to the** NIH IT Service Desk all lost or stolen NIH-issued equipment; known or suspected security incidents, information security policy violations or compromises, or suspicious activity. Known or suspected security incidents include actual or potential loss of control or compromises (whether intentional or unintentional, of your login name and password), PII and other sensitive NIH information maintained or in possession of HHS/NIH or information processed by contractors and third parties on behalf of HHS/NIH.) Also notify your supervisor and your Information Systems Security Officer (ISSO).
- Follow my Institute/Center procedures for bringing government-owned equipment on foreign travel.
- Maintain awareness of risks involved with clicking on e-mail or text message web links;
- Only use approved methods for accessing HHS/NIH information and HHS/NIH information systems;
- Ensure important data is backed up.

Privacy

- Understand and consent to having no expectation of privacy while accessing HHS/NIH computers, networks, or email;
- Collect information from members of the public only as required by my assigned duties and permitted by the Privacy Act of 1974, the Paperwork Reduction Act, and other relevant laws;

- Release information to members of the public including individuals or the media only as allowed by the scope of my duties and the law;
- Refrain from accessing information about individuals unless specifically authorized and required as part of my assigned duties;
- Use PII and PHI only for the purposes for which it was collected, to include conditions set forth by stated privacy notices and published System of Records Notices;
- Ensure the accuracy, relevance, timeliness, and completeness of PII, as is reasonably necessary and to the extent possible, to assure fairness in making determinations about an individual.

Sensitive Information

- Treat computer, network and web application account credentials as private sensitive information and refrain from sharing accounts;
- Secure sensitive information, regardless of media or format, when left unattended;
- Keep sensitive information out of sight when visitors are present;
- Sanitize or destroy electronic media and papers that contain sensitive data when no longer needed, in accordance with NIH records management (contact your IC Records Management Officer for questions) and the NIH Media Sanitization and Disposal Guidance, or as otherwise directed by management.
- Access sensitive information only when necessary to perform job functions; and
- Properly protect (e.g., encrypt) HHS/NIH sensitive information at all times while stored or in transmission, in accordance with the HHS Standard for Encryption of Computer Devices.

I must not:

- Violate, direct, or encourage others to violate HHS/NIH policies or procedures;
- Circumvent security safeguards, including violating security policies or procedures or reconfiguring systems, except as authorized;

- Use another personâ€™s account, identity, password/passcode/PIN, or PIV card or share my password/passcode/PIN;
- Remove data or equipment from the agency premises without proper authorization;
- Use HHS/NIH information, systems, and hardware to send or post threatening, harassing, intimidating, or abusive material about others in public or private messages or forums;
- Exceed authorized access to sensitive information;
- Share or disclose sensitive information except as authorized and with formal agreements that ensure third-parties will adequately protect it;
- Download or store sensitive information on personally-owned equipment;
- Transport, transmit, email, remotely access, or download sensitive information, inclusive of PII, unless such action is explicitly permitted by the manager or owner of such information and appropriate safeguards are in place per NIH policies concerning sensitive information;
- Use sensitive information for anything other than the purpose for which it has been authorized;
- Access information for unauthorized purposes;
- Use sensitive HHS/NIH data for private gain or to misrepresent myself or HHS/NIH or for any other unauthorized purpose;
- Store sensitive information in public folders or other insecure physical or electronic storage locations;
- Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information;
- Copy or distribute intellectual property including music, software, documentation, and other copyrighted materials without written permission or license from the copyright owner;
- Modify or install software without prior management approval;
- Use unauthorized external information systems (such as personal email or personal online storage accounts), equipment, or services to conduct any NIH/HHS business.
- Use systems (either government issued or non-government) without the following protections in place to access sensitive HHS/NIH information:
    - Antivirus software with the latest updates;
    - Anti-spyware and personal firewalls;

- A time-out function that requires re-authentication after no more than 30 minutes of inactivity on remote access; and
- Approved encryption to protect sensitive information stored on recordable media, including laptops, USB drives, and external disks; or transmitted or downloaded via email or remote connections.

I must refrain from the following activities when using federal government systems, which are prohibited per the HHS Policy for Personal use of Information Technology Resources.

- Unethical or illegal conduct;
- Sending or posting obscene or offensive material;
- Sending or forwarding chain letters, email spam, inappropriate messages, or unapproved newsletters and broadcast messages;
- Sending messages supporting prohibited partisan political activity as restricted under the Hatch Act;
- Conducting any commercial or for-profit activity;
- Using peer-to-peer (P2P) software except for secure tools approved in writing by the NIH CIO to meet business or operational needs;
- Sending, retrieving, viewing, displaying, or printing sexually explicit, suggestive text or images, or other offensive material;
- Creating and/or operating unapproved Web sites or services;
- Allowing personal use of HHS/NIH resources to adversely affect HHS/NIH systems, services, and co-workers (such as using non-trivial amounts of storage space or bandwidth for personal digital photos, music, or video);
- Using the Internet or NIH workstation to play games or gamble; and
- Posting HHS/NIH information to external newsgroups, social media and other types of third-party website applications, or other public forums without authority, including information which is at odds with HHS/NIH missions or positions. This includes any use that could create the perception that the

communication was made in my official capacity as a federal government employee, unless I have previously obtained appropriate HHS/NIH approval.

Federal Acknowledgement Statement

I have read the NIH Rules of Behavior, and understand and agree to comply with its provisions.

- I understand that when accessing a U.S. Government information system (which includes: 1) the computer, 2) the computer network, 3) all computers connected to that network, and 4) all devices and storage media attached to that network or to a computer on that network), use of the system is for U.S. Government-authorized use only. By using the information system, I understand and consent to the following:
    - I have no reasonable expectation of privacy regarding any communications or data transiting or stored on the information system, including removable storage media in my possession or work spaces. At any time, and for any lawful Government purpose, the government may monitor, intercept, record, and search and seize any communication or data transiting or stored on the information system or contained in removable storage media.
    - Any communication or data transiting or stored on the information system may be disclosed or used for any lawful Government purpose.
- I understand that violations of the NIH Rules or information security policies and standards may lead to disciplinary action, up to and including termination of employment; removal or debarment from work on Federal contracts or projects; and/or revocation of access to Federal information, information systems, and/or facilities and may also include civil and criminal penalties and/or imprisonment.
- I understand that exceptions to the NIH Rules must be authorized in advance in writing by the NIH Chief Information Officer or his/her designee.
- I also understand that violation of laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the Rules draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

Last Revised: 4/12/2018