Rules of Behavior for General Users v. 2.2

These *Rules of Behavior (RoB) for General Users* apply to all Department of Health and Human Services (HHS) employees, contractors, and other personnel who have access to HHS information resources and information technology (IT) systems. Users of HHS information and information systems shall read, acknowledge, and adhere to the following rules prior to accessing data and using HHS information and systems.

A. HHS Information Systems

When using and accessing HHS information resources and systems, I understand that I must:

1. Comply with federal laws, regulations, and HHS/Operating Division (OpDiv) policies, standards, and procedures and that I must not violate, direct or encourage others to violate HHS policies, standards or procedures;
2. Not allow unauthorized use and access to HHS information and information systems;
3. Not circumvent or bypass security safeguards, policies, systems' configurations, or access control measures unless authorized in writing;
4. Limit personal use of information and IT Resources to the extent that it does not:
   a. disrupt my productivity,
   b. interfere with the mission or operations of HHS, and
   c. violate HHS security and privacy policies;
5. Have no expectation of privacy while using and accessing HHS information resources and assets at any time, and I understand that any actions and activities are subject to HHS monitoring, recording, and auditing;
6. Complete all mandatory training (e.g., security and privacy awareness, role-based training, etc.) prior to accessing HHS systems and periodically thereafter as required by HHS policies;
7. Be accountable for my actions while accessing and using HHS information, information systems and IT resources;
8. Not share passwords or provide passwords to anyone, including system administrators. I must protect my passwords, Personal Identity Verification (PIV) card, Personal Identification Numbers (PIN) and other access credentials from disclosure and compromise;
9. Promptly change my password when required by HHS policy and if I suspect that it has been compromised;
10. Not use another person's account, identity, password/passcode/PIN, or PIV card or allow others to use my GFE and/or other HHS information resources provided to me to perform my official work duties and tasks;
11. Not reconfigure systems and modify GFE, install/load unauthorized/unlicensed software or make configuration changes without proper official authorization;
12. Properly secure all GFE, including laptops, mobile devices, and other equipment that store, process, and handle HHS information, when leaving them unattended either at the office and other work locations, such as home, hoteling space, etc. and while on travel. This includes locking workstations, laptops, placing GFE in locked drawer, cabinet, or simply out of plain sight, and removing my PIV card from my workstation.
13. Only use authorized credentials, including PIV card, to access HHS systems and facilities and will not attempt to bypass access control measures; and

14. Report all suspected and identified information security incidents and privacy breaches to the Helpdesk, Incident Response Team (IRT) and/or Privacy Incident Response Team (PIRT) as soon as possible, without unreasonable delay and no later than within ***one (1) hour*** of occurrence/discovery.[1]

B. Internet and Email

When accessing and using the Internet and email, I understand that I must:

1. Not access HHS/OpDiv Webmail from the public Internet;
2. Not use personal email and storage/service accounts to store/transmit HHS data and conduct HHS business;
3. Not use personal devices to conduct HHS business unless authorized by HHS/OpDiv Official;
4. Limit access to personal social media and networking sites (such as YouTube, Twitter, Facebook, etc.) while utilizing GFE and during official working hours and to the extent that it does not:
   a. disrupt my productivity,
   b. interfere with the mission or operations of HHS, and
   c. violate HHS security and privacy policies;
5. Limit activities during official work hours, which may adversely affect the security of HHS information, services, information systems, coworkers or cause network degradation (e.g., using social media, large amounts of storage space or bandwidth for personal reasons, such as digital photos, music, or video, using HHS email to create personal sites or subscribe to personal services and memberships, etc.);
6. Not click on links or open attachments sent via email or text message Web links from untrusted sources and verify information from trusted sources before clicking attachments;
7. Not auto-forward HHS email to external and internal email sources;
8. Not provide personal or official HHS information to an unsolicited email. If an email is received from any source requesting personal or organizational information or asking to verify accounts or security settings, I will report the incident to the Helpdesk and/or the Computer Security Incident Response Center (CSIRC)/Computer Security Incident Response Team (CSIRT) immediately;
9. Not connect GFE or contractor-owned equipment to unsecured Wi-Fi networks (e.g. airports, hotels, restaurants, etc.) and public Wi-Fi to conduct HHS business unless the Wi-Fi is at a minimum password protected;
10. Not upload or disseminate information which is at odds with departmental missions or positions or without proper authorization, which could create the perception that the communication was made in my official capacity as a federal government employee or contractor; and
11. Only disseminate authorized HHS information related to my official job and duties at HHS to internal and external sources.

C. Data Protection

When handling and accessing HHS information, I understand that I must:

[1] CSIRC and IRT points of contact are available at: https://intranet.hhs.gov/it/cybersecurity/hhs_csirc/index.html. Provide all necessary information that will help with the incident investigation.

1. Take all necessary precautions to protect HHS information and IT assets, including but not limited to hardware, software, sensitive information, including but not limited to Personally Identifiable Information (PII), Protected Health Information (PHI), federal records [media neutral], and other HHS information from unauthorized access, use, modification, destruction, theft, disclosure, loss, damage, or abuse, and in accordance with HHS policies[2];
2. Protect sensitive information (e.g., sensitive information, such as confidential business information, PII, PHI, financial records, proprietary data, etc.) at rest (stored on laptops or other computing devices) regardless of media or format, from disclosure to unauthorized persons or groups. This includes, but is not limited to:
    a. Never store sensitive information in public folders, unauthorized devices/services or other unsecure physical or electronic locations,
    b. Always encrypt sensitive information and in transit (transmitted via email, attachment, media, etc.),
    c. Always disseminate passwords and encryption keys out of band (e.g., via text message, in person, or phone call) or store password and encryption keys separately from encrypted files, devices and data when sending encrypted emails or transporting encrypted media,
    d. Access or use sensitive information only when necessary to perform job functions, and do not access or use sensitive information for anything other than authorized purposes, and
    e. Securely dispose of electronic media and papers that contain sensitive data when no longer needed, in accordance with the HHS Policy for Records Management and federal guidelines;
3. Immediately report all suspected and known security incidents (e.g., GFE loss or compromise, violation of security policies, etc.), privacy breaches (e.g., loss, compromise or unauthorized access and use of PII/PHI), and suspicious activities to the Helpdesk and/or CSIRC/CSIRT pursuant to HHS incident response policy and/or procedures[3];
4. Review Office of Security and Strategic Information (OSSI) requirements and policy on use of GFE during foreign travel prior to traveling abroad with GFE or to conduct HHS business; and
5. Notify my Personnel Security Representative (PSR) when there is a need to bring GFE on foreign travel (per requirements defined by the OSSI).

D. **Privacy**

I understand that I must:

1. Collect information about individuals only as required by my assigned duties and authorized by a program-specific law, after complying with any applicable notice or other requirements of laws such as the Privacy Act of 1974, the Paperwork Reduction Act, and agency privacy policies and OMB memoranda, such as OMB Memorandum M-17-06 governing collection of PII on agency websites;
2. Release information to members of the public (including individuals, organizations, the media, individual Members of Congress, etc.) only as allowed by the scope of my duties, applicable HHS policies, and the law;
3. Not access information about individuals unless specifically authorized and required as part

[2] HHS IT assets are defined as hardware, software, systems, services, and related technology assets used to execute work on behalf of HHS. This definition is adapted from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Revision 1, *Guide for Conducting Risk Assessments*

[3] Please review the OMB M-17-12 for the specific distinctions between incident response and breach response.

of my assigned duties;
4. Not use non-public HHS data for private gain or to misrepresent myself or HHS or for any other unauthorized purpose;
5. Use information about individuals (including PII[4] and PHI[5]) only for the purposes for which it was collected and consistent with conditions set forth in stated privacy notices such as those provided to individuals at the point of data collection or published in the *Federal Register* (to include System of Records Notices [SORNs]);
6. Ensure the accuracy, relevance, timeliness, and completeness of information about individuals, as is reasonably necessary and to the extent possible, to assure fairness in making determinations about an individual; and
7. Maintain no record describing how an individual exercises his or her First Amendment rights, unless it is expressly authorized by statute or by the individual about whom the record is maintained, or is pertinent to and within the scope of an authorized law enforcement activity.

E. **Strictly Prohibited Activities**

When using federal government systems and equipment, I must refrain from the following activities, which are strictly prohibited:

1. Conducting official HHS business using personal email or personal online storage/service account;
2. Using personal devices to conduct HHS business without written official authorization;
3. Unethical or illegal conduct (e.g. pornography, criminal and terrorism activities, and other illegal actions and activities);
4. Sending or forwarding chain letters, e-mail spam, inappropriate messages, or unapproved newsletters and broadcast messages except when forwarding to report this activity to authorized recipients;
5. Sending messages supporting or opposing partisan political activity as restricted under the Hatch Act and other federal laws and regulations;
6. Using peer-to-peer (P2P) software except for secure tools approved in writing by the OpDiv CIO (or designee) to meet business or operational needs;
7. Sending, retrieving, viewing, displaying, or printing sexually explicit, suggestive or pornographic text or images, or other offensive material (e.g. vulgar material, racially offensive material, etc.);
8. Creating and/or operating unapproved/unauthorized Web sites or services;
9. Using, storing, or distributing, unauthorized copyrighted or other intellectual property;
10. Using HHS information, systems, and devices to send or post threatening, harassing,

---

[4] PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. For other examples see: https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf

[5] Protected Health Information, as defined in the HIPAA Privacy Rule, is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition;
- the provision of health care to the individual;
- the past, present, or future payment for the provision of health care to the individual; and/or
- individual's information for which there is a reasonable basis to believe that it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g. name, address, birth date, Social Security Number)
  (available at: https://www.hhs.gov/hipaa/for-professionals/privacy).

intimidating, or abusive material about anyone in public or private messages or any forums;
11. Exceeding authorized access to sensitive information;
12. Using HHS GFE for commercial or for-profit activity, shopping, instant messaging (for unauthorized and non-work related purposes), playing games, gambling, watching movies, accessing unauthorized sites, and hacking;
13. Using an official HHS e-mail address to create personal commercial accounts for the purpose of receiving notifications (e.g., sales discounts, marketing, etc.), setting up a personal business or website, and signing up for personal memberships. Professional groups or memberships related to job duties at HHS are permissible;
14. Removing data or equipment from the agency premises without proper authorization;
15. Sharing, storing, or disclosing sensitive information with third-party organizations and/or using third-party applications (e.g. DropBox, Evernote, iCloud, etc.) unless authorized and with formal agreement in accordance with HHS policies;
16. Transporting, transmitting, e-mailing, texting, remotely accessing, or downloading sensitive information unless such action is explicitly permitted in writing by the manager or owner of such information and appropriate safeguards are in place per HHS policies concerning sensitive information; and
17. Knowingly or willingly concealing, removing, mutilating, obliterating, falsifying, or destroying HHS information.

SIGNATURE

I have read the above *RoB for General Users*, and understand and agree to comply with the provisions stated herein. I understand that violations of these RoB or HHS information security policies and standards may result in disciplinary action and that these actions may include termination of employment; removal or debarment from work on federal contracts or projects; revocation of access to federal information, information systems, and/or facilities; criminal penalties; and/or imprisonment.

I understand that exceptions to these RoB must be authorized in advance in writing by the designated authorizing officials. I also understand that violation of federal laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the HHS RoB draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

User's Name: _____
(Print)

User's Signature: _____

Date Signed: _____