

**Office of the Chief Information Officer  
Office of the Assistant Secretary for Administration  
Department of Health and Human Services**

**HHS Rules of Behavior  
(For Use of HHS Information Technology Resources)**

**August 26, 2010**

<b>Project:</b>	HHS-OCIO Standard RoB
<b>Document Number:</b>	HHS-OCIO-2010-0002.001S

This HHS standard is effective immediately:

The Department of Health and Human Services (HHS) *Rules of Behavior* (HHS RoB) provides appropriate use of all HHS information technology resources for Department users, including Federal employees, contractors, and other system users. The HHS RoB, in conjunction with the HHS-OCIO (2006-0001) *Policy for Personal Use of Information Technology Resources*, dated February 17, 2006, and are issued under the authority of the HHS-OCIO (2009-0003) *Policy for Information Systems Security and Privacy*, dated June 25, 2009. Both policy references are located at <http://www.hhs.gov/ocio/policy/index.html>. The HHS-OCIO-2008-0003.001S, HHS *Rules of Behavior*, dated February 12, 2008, is obsolete by this issuance which adds a signature page for Privileged User accounts.

All users of HHS information technology resources must read these rules and sign the accompanying acknowledgement form before accessing Department data/information, systems and/or networks. This acknowledgement must be signed annually, preferably as part of the HHS Information Systems Security Awareness Training, to reaffirm knowledge of, and agreement to adhere to the HHS RoB. The HHS RoB may be presented to the user in writing or electronically, and the user's acknowledgement may be obtained by written or electronic signature. Each Operating Division (OPDIV) Chief Information Officer (CIO) shall determine how signatures are to be submitted, retained, and recorded<sup>1</sup>; and may append any necessary information or fields to the signature page. For electronic signatures, the specific version number of the HHS RoB must be retained, along with the date and sufficient identifying information to uniquely link the signer to his or her corresponding information system accounts. Electronic copies of the signed signature page may be retained in lieu of the original. Each OPDIV CIO shall ensure that information system and information access is prohibited in the absence of a valid, signed acknowledgement of the HHS RoB from each user.

These rules cannot account for every possible situation. Therefore, personnel shall use their best judgment and highest ethical standards to guide their actions.

Non-compliance with the HHS RoB may be cause for disciplinary actions. Depending on the severity of the violation and management discretion, consequences may include one or more of the following actions:

- Suspension of access privileges; revocation of access to federal information, information systems, and/or facilities;
- Reprimand;
- Termination of employment;
- Removal or debarment from work on Federal contracts or projects;
- Monetary fines; and/or
- Criminal charges that may result in imprisonment.

HHS OPDIVs may require users to acknowledge and comply with OPDIV-level policies and requirements, which may be more restrictive than the rules prescribed herein.

---

<sup>1</sup> A privacy impact assessment (PIA) is required for collecting this information. The PIA should be used in determining if a System of Records Notice (SORN) is required. See *HHS Policy for Privacy Impact Assessment (PIA)*, located at: <http://www.hhs.gov/ocio/policy/index.html>.

Furthermore, supplemental rules of behavior may be created for specific systems which require users to comply with rules beyond those contained in this document. In such cases, users must also sign these supplemental rules of behavior prior to receiving access to these systems, and must comply with any ongoing requirements of each individual system to retain access (such as re-acknowledging the system-specific rules by signature each year). System owners shall document system-specific rules of behavior and any recurring requirement to sign the respective acknowledgement in the Security Plan for their systems. Each OPDIV CIO shall implement a process to obtain and retain the signed rules for such systems and shall ensure that user access to such system information is prohibited without a signed acknowledgement of system-specific rules and a signed acknowledgement of the HHS RoB.

National security systems, as defined by the Federal Information Security Management Act (FISMA), must independently or collectively implement their own system-specific rules.

These HHS RoB apply to local, network, and remote use<sup>2</sup> of HHS information (in both electronic and physical forms) and information systems by any individual.

I assert my understanding that:

- Information and system use must comply with Department and OPDIV policies and standards, and with applicable laws;
- Use for other than official, assigned duties is subject to the HHS-OCIO-2006-0001, *Policy for Personal Use of IT Resources*, dated February 17, 2006;
- Unauthorized access to information or information systems is prohibited; and
- Users must prevent unauthorized disclosure<sup>3</sup> or modification of sensitive information.<sup>3</sup>

I shall:

- Ensure that software, including downloaded software, is properly licensed, free of malicious code, and authorized before installing and using it on HHS systems;
- Abstain from loading unapproved software from unauthorized sources<sup>4</sup> on Department systems or networks;
- Wear identification badges at all times in Federal facilities;
- Log-off or lock systems when leaving them unattended;
- Use provisions for access restrictions and unique identification to information and avoid sharing accounts;
- Complete security awareness training before accessing any HHS system and on an annual basis thereafter, and complete any specialized role-based security or privacy training, as required by HHS policies;
- Permit only authorized HHS users to use HHS equipment and/or software;
- Secure sensitive information (media neutral) when left unattended;

---

<sup>2</sup> Refer to the Glossary of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems*, dated August 2009, for definitions of local, network, and remote access.

<sup>3</sup> HHS definition of sensitive information is defined in the HHS Memorandum: *Updated Departmental Standard for the Definition of Sensitive Information* (as amended) available at: [http://intranet.hhs.gov/infosec/policies\\_memos.html](http://intranet.hhs.gov/infosec/policies_memos.html).

<sup>4</sup> An unauthorized source is any location (e.g., file store or server to which a device could connect, Internet site, Intranet site) or process that is not permitted by HHS or OPDIV/STAFFDIV IT security personnel for the distribution of software.

- 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 the HHS-OCIO-2007-0004, *Policy for Records Management*, dated January 30, 2008 and sanitization policies, or as otherwise directed by management;
- Only access sensitive information necessary to perform job functions (i.e., need to know);
- Use Personally Identifiable Information (PII) 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, to assure fairness in making determinations about an individual;
- Adequately protect any sensitive information entrusted to me;
- Protect HHS information assets<sup>5</sup> (HHS assets include but are not limited to hardware, software, and federal records) from unauthorized access, use, modification, destruction, theft, or disclosure and shall treat such assets in accordance with any information handling policies;
- Properly protect (i.e., encrypt) HHS sensitive information, to include sensitive information sent via email; and
- Immediately report to the OPDIV Chief Information Security Officer (CISO) all: lost or stolen HHS equipment from the agency premises without proper authorization; known or suspected security incidents; known or suspected information security policy violations or compromises; or suspicious activity in accordance with OPDIV procedures. Known or suspected security incidents involve the actual or potential loss of control or compromise, whether intentional or unintentional, of authenticator, password, or sensitive information maintained or in possession of HHS or information processed by contractors and third parties on behalf of HHS.

I shall **not**:

- Violate, direct, or encourage others to violate HHS policies or procedures;
- Circumvent security safeguards including violating security policies or procedures or reconfigure systems except as authorized (i.e., violation of least privilege);
- Use another person's account, identity, or password;
- Remove computers or equipment from the agency premises without proper authorization;
- Send or post threatening, harassing, intimidating, or abusive material about others in public or private messages or forums;
- Exceed authorized access to sensitive information;
- Store sensitive information in public folders or other insecure physical or electronic storage locations;
- Share or disclose sensitive information except as authorized and with formal agreements that ensure third parties will adequately protect it;
- Transport, transmit, email, remotely access, or download sensitive information unless such action is explicitly permitted by the manager or owner of such information and appropriate safeguards are in place per HHS policies concerning sensitive information;

---

<sup>5</sup> HHS IT assets are defined as hardware, software, systems, services, and related technology assets used to execute work on behalf of HHS. Definition is adapted from NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, dated July 2002.

- Use sensitive information for anything other than the purpose for which it has been authorized;
- Access information for unauthorized purposes;
- Use sensitive HHS data for private gain or to misrepresent myself or HHS or any other unauthorized purpose;
- Store sensitive information on mobile devices<sup>6</sup> such as laptops, personal digital assistants (PDAs), universal serial bus (USB) drives, or on remote/home systems without authorization and/or appropriate safeguards (i.e., HHS approved encryption);
- Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information for personal use for myself or others;
- Copy or distribute intellectual property—including music, software, documentation, and other copyrighted materials—without permission or license from the copyright owner;
- Modify or install software without prior management approval;
- Load unapproved software from unauthorized sources<sup>7</sup> on Department systems or networks;
- Use a personal email system (i.e., Gmail, Yahoo, Hotmail) to transmit sensitive information; and
- Use systems without the following protections engaged to access sensitive HHS information:
  - Antivirus software with the latest updates;
  - Anti-spyware and personal firewalls installed on personally-owned systems;
  - A time-out function that requires re-authentication after no more than 30 minutes of inactivity on remote access and mobile devices ; and
  - Approved encryption to protect sensitive information stored on mobile devices or recordable media, including laptops, USB drives, and external disks; stored on remote or home systems; or transmitted or downloaded via email or remote connections.

The following are prohibited on Federal Government systems per the HHS-OCIO-2006-0001 *Policy for Personal Use of Information Technology Resources*, dated February 17, 2006:

- Unethical or illegal conduct;
- Sending or posting obscene or offensive material in messages or forums;
- Sending or forwarding chain letters, email spam, inappropriate messages, or unapproved newsletters and broadcast messages;
- Sending messages supporting political activity restricted under the Hatch Act;
- Conducting any commercial or “for-profit” activity;
- Utilizing peer-to-peer software except for secure tools approved in writing by the OPDIV 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;
- Incurring more than minimal additional expense, such as using non-trivial amounts of storage space or bandwidth for personal files or photos; and
- Using the Internet or HHS workstation to play games, visit chat rooms, or gamble.

---

<sup>6</sup> Refer to the Glossary of NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems*, dated August 2009, for the definition of mobile device.

<sup>7</sup> Ibid.

I shall ensure passwords:

- Are complex, and contain a minimum of eight alphanumeric characters and at least one uppercase and one lowercase letter, one number, and one special character;
- Do not contain or consist of common words, names, or user IDs;
- Are changed immediately in the event of known or suspected compromise, and immediately upon system installation (e.g., default or vendor-supplied passwords);
- Are not reused until at least six other passwords have been used; and
- Are committed to memory, or stored in a secure place.

**SIGNATURE PAGE**

I have read the *HHS Rules of Behavior* (HHS RoB), version 2010-0002.001S, dated August 26 2010 and understand and agree to comply with its provisions. I understand that violations of the HHS RoB 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 criminal penalties and/or imprisonment. I understand that exceptions to the HHS RoB must be authorized in advance in writing by the OPDIV 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 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: \_\_\_\_\_

APPROVED BY AND EFFECTIVE ON:

\_\_\_\_\_/s/\_\_\_\_\_  
Michael W. Carleton  
HHS Chief Information Officer\_\_\_\_\_  
August 26, 2010  
DATE

The record copy is maintained in accordance with GRS 1, 18.a.

## Addendum: HHS Rules of Behavior for Privileged User Accounts

The HHS Rules of Behavior for Privileged User Accounts is an addendum to the *HHS Rules of Behavior* (HHS RoB) and provides common rules on the appropriate use of all HHS information technology resources for all Department privileged users, including Federal employees, interns, and contractors. Privileged User account roles have elevated privileges above those in place for general user accounts regardless of account scope (e.g., including both local and domain administrator accounts). Potential compromise of Privileged User accounts carries a risk of substantial damage and therefore privileged user accounts require additional safeguards. All users of Privileged accounts for Department information technology resources must read these rules and sign the accompanying acknowledgement form in addition to the HHS RoB before accessing Department data/information, systems and/or networks in a privileged role. The same signature acknowledgement process followed for the HHS (RoB) applies to the Privileged User accounts. Each OPDIV shall maintain a list of Privileged User accounts.

I understand that as a Privileged User<sup>8</sup>, I shall:

- Protect all Privileged account passwords on Low, Moderate, and High systems;
- Comply with all System/Network Administrator responsibilities in accordance with HHS policy;
- Use my Privileged User account(s) for official administrative actions only;
- Notify system owner immediately when privileged access is no longer required; and
- Complete any specialized role-based security or privacy training as required before receiving privileged system access.

I understand that as a Privileged User, I shall **not**:

- Share Privileged User account(s) or password(s);
- Install, modify, or remove any system hardware or software without system owner written approval;
- Remove or destroy system audit, security, event, or any other log data unless authorized by the system owner in writing;
- Acquire, possess, trade, or use hardware or software tools that could be employed to evaluate, compromise, or bypass information systems security controls;
- Introduce unauthorized code, Trojan horse programs, malicious code, or viruses into HHS information systems or networks;
- Knowingly write, code, compile, store, transmit, or transfer malicious software code, to include viruses, logic bombs, worms, and macro viruses;
- Use Privileged User account(s) for day-to-day communications;
- Elevate the privileges of any user without prior approval from the system owner;
- Use privileged access to circumvent HHS policies or security controls; or
- Use a Privileged User account for Web access except in support of administrative related activities.

---

<sup>8</sup> Per NIST 800-53 Rev. 3, privileged roles include, for example, key management, network and system administration, database administration, and Web administration.

**SIGNATURE PAGE**

I have read the Addendum: *HHS Rules of Behavior for Privileged User Accounts* (HHS RoB for Privileged User Account ) of the HHS Rules of Behavior, version 2010-0002.001S, dated August 26, 2010 and understand and agree to comply with its provisions. I understand that violations of the HHS RoB for Privileged User Account 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 criminal penalties and/or imprisonment. I understand that exceptions to the HHS RoB for Privileged User Account must be authorized in advance in writing by the OPDIV 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 HHS RoB for Privileged User Account draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

Privileged User's

Name: \_\_\_\_\_

(Print)

Privileged User's

Signature: \_\_\_\_\_

Date Signed: \_\_\_\_\_

APPROVED BY AND EFFECTIVE ON:

\_\_\_\_\_/s/\_\_\_\_\_  
 Michael W. Carleton  
 HHS Chief Information Officer

\_\_\_\_\_  
 August 26, 2010  
 DATE

The record copy is maintained in accordance with GRS 1, 18.a.