Rules of Behavior for Use of HHS Information Resources

July 24, 2013

This Department of Health and Human Services (HHS or Department) standard is effective immediately:

The *Rules of Behavior for Use of HHS Information Resources* (HHS RoB) provides the rules that govern the appropriate use of all HHS information resources for Department users, including federal employees, contractors, and other system users. The HHS RoB, in conjunction with the *HHS Policy for Personal Use of Information Technology Resources*[1] (as amended), are issued under the authority of the *Policy for Information Systems Security and Privacy (IS2P).*[2] The prior HHS RoB (dated August 26, 2010) is made obsolete by the publication of this updated version.

All new users of HHS information resources must read the HHS RoB and sign the accompanying acknowledgement form before accessing Department data or other information, systems, and/or networks. This acknowledgement must be completed annually thereafter, which may be done as part of annual HHS Information Systems Security Awareness Training. By signing the form users reaffirm their knowledge of, and agreement to adhere to, the HHS RoB. The HHS RoB may be presented to the user in hardcopy or electronically. The user's acknowledgement may be obtained by written signature or, if allowed per Operating Division (OpDiv) or Staff Division (StaffDiv) policy and/or procedure, by electronic acknowledgement or signature.

The HHS RoB cannot account for every possible situation. Therefore, where the HHS RoB does not provide explicit guidance, personnel must use their best judgment to apply the principles set forth in the standards for ethical conduct to guide their actions.[3]

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 disbarment 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. Supplemental rules of behavior may be created for specific systems[4] that 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 ongoing requirements of each individual system to retain access (such as re-acknowledging the system-specific rules by signature each year). System owners must document any additional system-specific rules of behavior and any recurring requirement to sign the respective acknowledgement in the security plan for their systems. Each OpDiv Chief Information Officer (CIO) must implement a process to obtain and retain the signed rules of behavior for such systems and must 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[5] of HHS information (in both electronic and physical forms) and information systems by any individual.

Users of HHS information and systems must acknowledge the following statements:

I assert my understanding that:

- Use of HHS information and systems must comply with Department and OpDiv policies, standards, and applicable laws;
- Use for other than official assigned duties is subject to the *HHS Policy for Personal Use of IT Resources*, (as amended);[6]
- Unauthorized access to information or information systems is prohibited; and
- Users must prevent unauthorized disclosure or modification of sensitive information.[7]

I must:

General Security Practices

- Follow HHS 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 information and information systems;
- Ensure that I have appropriate authorization to install and use software, including downloaded software on HHS 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 systems and facilities;
- Complete security awareness training (i.e., HHS Information Systems 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;[8]
- Permit only authorized HHS users to use HHS equipment and/or software;
- Take all necessary precautions to protect HHS information assets[9] (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 appropriate incident response organization or help desk (pursuant to OpDiv policy and/or procedures) all lost or stolen HHS equipment; known or suspected security incidents;[10] known or suspected information security policy violations or compromises; or suspicious activity in accordance with OpDiv procedures;

- Notify my OpDiv/StaffDiv Personnel Security Representative (PSR) when I plan to bring government-owned equipment on foreign travel (per requirements defined by the Office of Security and Strategic Information (OSSI));[11]
- Maintain awareness of risks involved with clicking on e-mail or text message web links; and
- Only use approved methods for accessing HHS information and HHS information systems.

Privacy

- Understand and consent to having no expectation of privacy while accessing HHS computers, networks, or e-mail;
- 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 and consistent with conditions set forth by stated privacy notices such as those provided to individuals at the point of data collection and published System of Records Notices; and
- 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 the *HHS Policy for Records Management*[12] and sanitization policies, or as otherwise lawfully directed by management;
- Access sensitive information only when necessary to perform job functions; and
- Properly protect (e.g., encrypt) HHS sensitive information at all times while stored or in transmission, in accordance with the *HHS Standard for Encryption of Computing Devices*.[13]

I must **not**:

- Violate, direct, or encourage others to violate HHS policies or procedures;
- Circumvent security safeguards, including violating security policies or procedures or reconfiguring systems, except as authorized;
- Use another person'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 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;
- Transport, transmit, e-mail, 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;
- 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 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 proper approval per OpDiv procedures;
- Conduct official government business or transmit/store sensitive HHS information using non-authorized equipment or services; or
- Use systems (either government issued or non-government) without the following protections in place to access sensitive HHS 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[14] to protect sensitive information stored on recordable media, including laptops, USB drives, and external disks; or transmitted or downloaded via e-mail 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,*[15] (as amended):

- Unethical or illegal conduct;
- Sending or posting obscene or offensive material;
- Sending or forwarding chain letters, e-mail spam, inappropriate messages, or unapproved newsletters and broadcast messages;
- Sending messages supporting prohibited partisan political activity as restricted under the Hatch Act;[16]
- Conducting any commercial or for-profit activity;
- 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;
- 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 resources to adversely affect HHS 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 HHS workstation to play games or gamble; and
- Posting Department information to external newsgroups, social media and/or other types of third-party website applications,[17] or other public forums without authority, including information which is at odds with departmental 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 Department approval.

APPROVED BY AND EFFECTIVE ON:

/s/	July 24, 2013
Frank Baitman	DATE
HHS Chief Information Officer	

SIGNATURE PAGE

I have read the *HHS Rules of Behavior for Use of Information Resources* (HHS RoB), document number HHS-OCIO-2013-0003S and dated July 24, 2013, 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 and that these actions may include termination of employment; removal or disbarment 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 the HHS RoB must be authorized in advance in writing by the Operating Division (OpDiv) Chief Information Officer or his/her designee. I also understand that violation of certain 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: _____

Digital Signature (optional):

The record copy is maintained in accordance with the General Records Schedule (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 for Use of Information Resources* (HHS RoB) and provides common rules on the appropriate use of all HHS information technology resources for all Department Privileged Users,[18] 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., 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 User accounts for Department information technology resources must read these standards 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 Operating Division (OpDiv) must maintain a list of Privileged User accounts.

I understand that as a Privileged User, I must:

- Protect all Privileged User account passwords/passcodes/Personal Identity Verification (PIV) personal identified numbers (PINs) 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 owners 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 must **not**:

- Share Privileged User account(s) or password(s)/passcode(s)/PIV PINs;
- 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;
- 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;
- Use a Privileged User account for Web access except in support of administrative related activities; or
- Modify security settings on system hardware or software without the approval of a system administrator and/or a system owner.

SIGNATURE PAGE

I have read the *HHS Rules of Behavior for Privileged User Accounts* (addendum to the HHS Rules of Behavior (HHS RoB), document number HHS-OCIO-2013-0003S and dated July 24, 2013), and understand and agree to comply with its provisions. I understand that violations of the *HHS Rules of Behavior for Privileged User Accounts* or information security policies and standards may lead to disciplinary action and that these actions may include termination of employment; removal or disbarment 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 the *HHS Rules of Behavior for Privileged User Accounts* must be authorized in advance in writing by the OpDiv Chief Information Officer or his/her designee. I also understand that violation of certain laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the *HHS Rules of Behavior for Privileged User Accounts* 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: _____

Digital Signature (optional):

The record copy is maintained in accordance with General Records Schedule (GRS) 1, 18.a.

[1] Available at: http://www.hhs.gov/ocio/policy/index.html

[2] Available at: http://www.hhs.gov/ocio/policy/index.html

[3] Refer to the Employee Standards of Conduct published by the U.S. Office of Government Ethics, available at: http://www.oge.gov/Laws-and-Regulations/Employee-Standards-of-Conduct/Employee-Standards-of-Conduct

[4] National Institute of Standards and Technology (NIST) Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, defines an "information system" as: "A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."

[5] Refer to the glossary of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations for definitions of local, network, and remote access.

[6] Available at: http://www.hhs.gov/ocio/policy/index.html.

[7] HHS Memorandum: Updated Departmental Standard for the Definition of Sensitive Information (as amended) is available at: http://intranet.hhs.gov/it/cybersecurity/policies/index.html.

[8] HHS Memorandum: Role-Based Training (RBT) of Personnel with Significant Security Responsibilities (available at: http://intranet.hhs.gov/it/cybersecurity/policies/index.htmldefines the types of positions requiring specialized training.

[9] 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 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Revision 1, Guide for Conducting Risk Assessments.

[10] 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 by or in the possession of HHS or information processed by contractors and third-parties on behalf of HHS.

[11] OSSI policies for foreign travel can be found at: http://intranet.hhs.gov/security/ossi/foreign/index.html

[12] Available at: http://www.hhs.gov/ocio/policy/index.html

[13] Available at: http://intranet.hhs.gov/it/cybersecurity/policies/index.html

[14] Refer to the HHS Standard for Encryption of Computing Devices, available at: http://intranet.hhs.gov/it/cybersecurity/policies/index.html.

[15] Available at: http://www.hhs.gov/ocio/policy/index.html.

[16] For additional guidance refer to http://www.osc.gov/hatchact.htm and 5 C.F.R. Part 2635: Standards of ethical conduct for employees of the executive branch.

[17] Refer to the HHS Policy for Managing the Use of Third-Party Websites and Applications, available at http://www.hhs.gov/ocio/policy/index.html.

[18] Per National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, privileged roles include, for example, key management, network and system administration, database administration, and Web administration.

Content created by Office of the Chief Information Officer (OCIO)

Content last reviewed on September 16, 2017