

**Department of Health and Human Services Centers for Medicare & Medicaid Services Center for Clinical Standards and Quality Information Systems Group**

**7500 Security Boulevard**

**Baltimore, Maryland 21244-1850**

Healthcare Quality Information System (HCQIS)

Rules of Behavior (RoB)

Version 2.1

11 February 2021

**Revision/Change Record**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Version | Description | Page, Section Affected | Editor |
| August 2018 | 1.0 | Initial Version | All | Brandon Tennessee (CMS) |
| April 2019 | 2.0 | Updated e-mail/Snow Security Violation TableSignature to acknowledge RoB. –Cloud verbiage updatedAdded Elevated User Account RoB | 2.3.2 & 2.4.1, 2.4.2& Appendix A, B and C | Brandon Tennessee(CMS) |
| September 2019 | 2.0 | Total revision of document, based on HHS Rules of Behavior | All | Ian Sheldon (CMS)Maureen Fisher (Ventech Solutions) |
| October 2019 | 2.0 | Signatures | 2 | Ian Sheldon |
| February 2021 | 2.1 | Updated Strictly ProhibitedActivities section | 6 | Malisa Anderson(Ventech Solutions) |

Contents

[Introduction](#_bookmark0) [1](#_bookmark0)

1. [Purpose](#_bookmark1) [1](#_bookmark1)
2. [Standard Rules of Behavior](#_bookmark2) [1](#_bookmark2)
3. [Information and Assistance](#_bookmark3) [2](#_bookmark3)
4. [Effective Date/Implementation](#_bookmark4) [2](#_bookmark4)
5. [Approved](#_bookmark5) [2](#_bookmark5)

[Appendix A: Rules of Behavior for General Users](#_bookmark6) [3](#_bookmark6)

[Appendix B: Rules of Behavior for Privileged Users](#_bookmark7) [7](#_bookmark7)

[Appendix C: Applicable Laws and Further Guidance](#_bookmark8) [9](#_bookmark8)

[Legislative](#_bookmark9) [9](#_bookmark9)

[OMB Guidance](#_bookmark10) [9](#_bookmark10)

[CMS Guidance](#_bookmark11) [9](#_bookmark11)

[HHS Guidance](#_bookmark12) [9](#_bookmark12)

# Introduction

The Healthcare Quality Information System (HCQIS) Rules of Behavior (RoB) specifies the rules that govern the appropriate use and protection of all HCQIS information and IT resources to ensure the security and privacy of information technology (IT) equipment, systems, and data as well as their confidentiality, integrity, and availability. This policy applies in addition to the [HHS Rules Of Behavior,](https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/hhs-rules-of-behavior-for-the-use-of-hhs-information-and-it-resources-policy.html) to which all HCQIS contractors and other HCQIS information system users are bound, and is issued under the authority of the [CMS](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html) [Information Systems Security and Privacy Policy (IS2P2).](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html)

# Purpose

The RoB rescinds and replaces the QualityNet Rules of Behavior V.1.0, August 2018. It includes baseline requirements for two types of users: General Users and Privileged Users. The RoB applies to all users of HCQIS information and IT resources whether working at their primary duty station, while teleworking, at a satellite site or any other alternative workplaces, and while traveling.

# Standard Rules of Behavior

RoB are provided for the following user types:

* 1. General users, see Appendix A.
	2. Privileged users see Appendix B. Privileged users must read and sign both documents.

All HCQIS contractors and other personnel with access to HCQIS information and IT systems shall read, acknowledge, and adhere to the General User RoB prior to accessing and using HCQIS information resources and IT systems. This acknowledgement shall be completed:

1. At HCQIS onboarding or prior to start of work on a HCQIS contract, grant, or other agreement, and
2. At least annually thereafter, and/or in combination with CMS information cybersecurity awareness training.

All privileged users (e.g., network/system administrators, developers, etc.) shall read, acknowledge, and adhere to the HCQIS Privileged User RoB prior to obtaining a privileged user account, and at least annually thereafter.

#### Non-Compliance

This RoB cannot account for every possible situation. Therefore, where this policy does not provide explicit guidance, personnel shall use their best judgment to guide their actions and seek guidance when appropriate from their CMS Contracting Officer’s Representative (COR) or their Information Systems Security Officer (ISSO).

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

1. Mandatory security training
2. Suspension of access privileges.
3. Revocation of access to federal information, information systems, and/or facilities.
4. Reprimand.
5. Termination of employment.
6. Removal or disbarment from work on federal contracts or projects.
7. Monetary fines; and/or
8. Criminal charges that may result in imprisonment.

# Information and Assistance

Submit any questions, comments, suggestions, or requests for further information to the [HCQIS Feedback](https://hcqis.sharepoint.com/sites/Security/Lists/Feedback%20Form?viewpath=%2Fsites%2FSecurity%2FLists%2FFeedback%20Form) [Form.](https://hcqis.sharepoint.com/sites/Security/Lists/Feedback%20Form?viewpath=%2Fsites%2FSecurity%2FLists%2FFeedback%20Form)

# Effective Date/Implementation

The effective date of this Policy is 14 October 2019.

# Approved

### Steven R. Davidson -S

Steve Davidson Director

Digitally signed by Steven

R. Davidson -S Date: 2019.10.11 13:41:37 -04'00'

Information Systems Group

Center for Clinical Standards and Quality Centers for Medicare and Medicaid Services

Digitally signed by Seth R. Thomas III -S

Seth R.

Date: 2019.10.10

Thomas III -S

14:00:20 -04'00'

Seth Thomas Director

Information Systems Security Staff Center for Clinical Standards and Quality

Centers for Medicare and Medicaid Services

# Appendix A: Rules of Behavior for General Users

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

#### HCQIS Information Systems

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

* 1. Comply with federal laws, regulations, and CMS policies, standards, and procedures, and that I must not violate, direct, or encourage others to violate CMS policies, standards, or procedures.
	2. Be accountable for my actions while accessing and using HCQIS information, information systems and IT resources.
	3. Not allow unauthorized use and access to HCQIS information and information systems.
	4. Only use authorized credentials. Not share passwords or provide passwords to anyone. Protect my password and other access credentials from disclosure and compromise.
	5. Not circumvent or bypass security safeguards, policies, system configurations, or access control measures unless authorized in writing.
	6. Ensure that the latest patches to my computer’s operating system (OS) have been applied, either through participating in my corporate patching process or having automatic updates enabled, or both.
	7. Ensure that my contractor-furnished equipment (CFE) has anti-virus software installed and is running the latest version of the anti-virus provider’s virus/malware signatures files.
	8. Ensure that any web browser I use is running at the browser’s latest version.
	9. Not record any webinar that I host which includes discussion or display of sensitive CMS/HCQIS information.
	10. Have no expectation of privacy while using and accessing HCQIS information resources at any time, and I understand that any actions and activities are subject to monitoring, recording, and auditing.
	11. Complete all mandatory training (e.g., security and privacy awareness, role-based training, Records Management, etc.) prior to accessing HCQIS systems and periodically thereafter as required by CMS policies.
	12. Promptly change my password when required by CMS or organizational policy, or if I suspect that it has been compromised.
	13. Not use another person’s account, identity, password, or passcode.
	14. Properly secure all equipment, including laptops, mobile devices, and other equipment that process, and handle HCQIS information, when leaving them unattended either at the office and other locations, such as home, hoteling space, etc. and while on travel. This includes locking workstations, laptops, placing equipment in a locked drawer, cabinet, or simply out of plain sight.
	15. Guard against unauthorized access to CMS information through “shoulder surfing”.
	16. Not perform contract work while outside of the United States.
	17. Immediately report all suspected and identified information security incidents (e.g., violation of security policies) and privacy breaches (e.g., loss, compromise or unauthorized access and use of PII/PHI) to your Security Point of Contact (SPOC) and by submitting a security Incident Response form to the Security Operations Center (SOC) via Managed File Transfer (MFT) or by encrypting the form and e-mailing it to the SOC (e-mail: soc@hcqis.org).
	18. Report all suspected and identified information security incidents (e.g., violation of security policies) and privacy breaches (e.g., loss, compromise or unauthorized access and use of PII/PHI) to my SPOC and/or the HCQIS Helpdesk, as soon as possible, without unreasonable delay and no later than within one (1) hour of occurrence/discovery. The HCQIS Helpdesk can provide all necessary information that will help with the incident investigation

#### Internet and Email

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

* 1. Follow CMS guidelines for handling (receiving) and transmitting sensitive information when approved to use corporate email in place of HCQIS email (see the HCQIS CFE Data Management Policy).
	2. Not auto-forward email to external or internal email sources.
	3. Not provide personal or official HCQIS information in response 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 my SPOC and/or the HCQIS Helpdesk immediately.
	4. Not connect equipment to unsecured Wi-Fi networks (e.g. airports, hotels, restaurants, etc.) and public Wi-Fi to conduct HCQIS business unless the Wi-Fi is, at a minimum, password protected.
	5. Only disseminate authorized HCQIS information related to my official job and duties to internal and external sources.
	6. Maintain awareness of potential phishing threats, reporting suspected phishing emails to SPAM@cms.hhs.gov

#### Data Protection

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

* 1. Take all necessary precautions to safeguard CMS information and IT systems, including but not limited to hardware, software, sensitive information, Personally Identifiable Information (PII), Protected Health Information (PHI), and other federal records and CMS information from unauthorized access, use, modification, destruction, theft, disclosure, loss, damage, or abuse;
	2. Not download HCQIS/CMS data to non-government furnished equipment (GFE), for example, external hard drives or USB drives.
	3. Protect sensitive information (e.g. confidential business information, PII, PHI, financial records, proprietary data, etc.) from disclosure to unauthorized persons or groups. This includes, but is not limited to:
		1. Access or use sensitive information only when necessary to perform job functions, and not access or use sensitive information for anything other than authorized purposes.
		2. Never store sensitive information in public folders, unauthorized devices/services or other unsecure physical or electronic locations, including online storage.
		3. Always encrypt sensitive information in transit (transmitted via email, attachment, media, etc.) using FIPS 140-2 approved encryption.
		4. 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; and
		5. Securely dispose of electronic media and papers that contain sensitive data when no longer needed. See [QualityNet Media Protection and Decommission Procedures](https://hcqis.sharepoint.com/sites/Security/SiteAssets/SitePages/Policies%20and%20Procedures/QualityNet%20Media%20Protection%20and%20Decommission%20Procedures%20V4.0-final.pdf) for details.

#### 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 CMS privacy policies and OMB memoranda, such as OMB Memorandum M-17-06 governing collection of PII on CMS 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/CMS policies, and the law.
3. Not access information about individuals unless specifically authorized and required as part of my assigned duties.
4. Not use non-public CMS data for private gain or to misrepresent myself or CMS or for any other unauthorized purpose.
5. Use information about individuals (including PII and PHI) 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).
	* 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.
	* PHI, as defined in the HIPAA Privacy Rule, is information, including demographic data, that relates to:
		+ an 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
		+ 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)
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.

#### Strictly Prohibited Activities

When using federal government systems, I must not engage in the following activities, which are strictly prohibited:

* + 1. Unethical or illegal conduct (e.g. pornography, criminal and terrorism activities, and other illegal actions and activities).
		2. 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.
		3. Using peer-to-peer (P2P) software except for secure tools approved in writing by the CMS CIO (or designee) to meet business or operational needs.
		4. 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.).
		5. Creating and/or operating unapproved/unauthorized Web sites or services.
		6. Using, storing, or distributing, unauthorized copyrighted or other intellectual property.
		7. Using HCQIS information systems to send or post threatening, harassing, intimidating, or abusive material about anyone in public or private messages or any forums.
		8. Exceeding authorized access to sensitive information.
		9. 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 CMS policies.
		10. Transporting, transmitting, e-mailing, texting, remotely accessing, or downloading sensitive information unless such action is explicitly permitted in writing by the owner of such

information and appropriate safeguards are in place per CMS policies concerning sensitive information; and

* + 1. Knowingly or willingly concealing, removing, mutilating, obliterating, falsifying, or destroying CMS information.
		2. The use of personal accounts with third party cloud storage providers (ex. Microsoft OneDrive, Dropbox, Google Drive) is prohibited.

#### SIGNATURE

I have read the above Rob for General Users, 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 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 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 these 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:

Appendix B: Rules of Behavior for Privileged Users

The following HCQIS Rules of Behavior (RoB) for Privileged Users is an addendum to the Rules of Behavior for General Users and provides mandatory rules on the appropriate use and handling of HCQIS information technology (IT) resources for all privileged users, including federal employees, interns, contractors, and other staff who possess privileged access to HCQIS information systems. Privileged users have network accounts with elevated privileges that grant them greater access to IT resources than non-privileged users. These privileges are typically allocated to system, network, security, and database administrators, as well as other IT administrators. The compromise of a privileged user account may expose CMS to a high level of risk; therefore, privileged user accounts require additional safeguards.

A Privileged User is a user who has been granted significantly elevated privileges for access to protected physical or logical resources. A privileged user has the potential to compromise the three security objectives of confidentiality, integrity, and availability. Such users include, for example, security personnel or system administrators who are responsible for managing shared IT resources and have been granted permissions to create new user accounts, modify user privileges, as well as make system changes. Examples of privileged users include:

1. Database administrator
2. Domain administrator
3. Data center operations personnel
4. IT tester/auditor
5. Helpdesk support and computer/system maintenance personnel
6. Network engineer
7. System administrator
8. Security personnel.

Privileged users shall read, acknowledge, and adhere to the RoB for Privileged Users and any other CMS policy or guidance for privileged users, prior to obtaining access and using HCQIS information and information systems and/or networks in a privileged role.

I understand that as a Privileged User, I must:

* Use Privileged User accounts appropriately for their intended purpose and only when required for official administrative actions.
* Protect all Privileged User account passwords/passcodes/ personal identified numbers (PINs) and other login credentials used to access HCQIS information systems.
* Comply with all system/network administrator responsibilities in accordance with the CMS IS2P2 and any other applicable policies.
* Notify system owners immediately when privileged access is no longer required.
* Properly protect all sensitive information and securely dispose of information that is no longer needed in accordance with CMS sanitization policies.
* Report all suspected and identified information security incidents (e.g., violation of security policies) and privacy breaches (e.g., loss, compromise or unauthorized access and use of PII/PHI) to my SPOC and/or the HCQIS Helpdesk, as soon as possible, without unreasonable delay and no later than within one (1) hour of occurrence/discovery. The HCQIS Helpdesk can provide all necessary information that will help with the incident investigation
* Immediately report all suspected and identified information security incidents (e.g., violation of security policies) and privacy breaches (e.g., loss, compromise or unauthorized access and use of PII/PHI) by submitting a security Incident Response form to the Security Operations Center (SOC) via Secure File Transfer (SFT) or by encrypting the form and e-mailing it to the SOC (e-mail: soc@hcqis.org); 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), password(s)/passcode(s), and another login credentials.
* Install, modify, or remove any system hardware or software without official written approval or unless it is part of my job duties.
* Remove or destroy system audit logs or any other security, event log information unless authorized by appropriate official(s) in writing.
* Tamper with audit logs of any kind. Note: In some cases, logs can be considered evidence and tampering may be a criminal offense punishable by fines and possible imprisonment.
* Acquire, possess, trade, or use hardware or software tools that could be employed to evaluate, compromise, or bypass information systems security controls for unauthorized purposes.
* Introduce unauthorized code, malicious code, viruses, or other malicious software into HCQIS 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 and other non-privileged transactions and activities.
* Elevate the privileges of any user without prior approval.
* Use privileged access to circumvent CMS policies or security controls.
* Access information outside of the scope of my specific job responsibilities or expose non-public information to unauthorized individuals.
* Use a Privileged User account for Web access except in support of administrative related activities.
* Modify security settings on system hardware or software without the approval of a system administrator and/or a system owner; and
* Use systems without the following protections in place to access sensitive CMS information:
1. Antivirus software with the latest updates,
2. Anti-spyware and personal firewalls,
3. A time-out function that requires re-authentication after no more than 15 minutes of inactivity on remote access, and
4. Approved encryption 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.

#### SIGNATURE

I have read the above Rules of Behavior (RoB) for Privileged 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 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 also understand that violation of federal laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which these 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:

# Appendix C: Applicable Laws and Further Guidance

## Legislative

1. [Federal Information Security Modernization Act of 2014 (FISMA) - PDF,](https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf) Pub. L. No. 113-283, 128 Stat. 3073, codified at 44 U.S.C. Chapter 35, Subchapter II
2. [5 U.S.C. Section 552a (the Privacy Act)](https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition)

## OMB Guidance

1. OMB Memorandum M-17-12, [Preparing for and Responding to a Breach of Personally Identifiable Information - PDF](https://www.safcioa6.af.mil/Portals/64/documents/Resources/OMB%20M%2017-12%20-%20Infographic%20v2.pdf?ver=2018-02-01-125646-093)

## CMS Guidance

* 1. [CMS Information Systems Security and Privacy Policy (IS2P2).](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/CIO-Directives-and-Policies/CIO-IT-Policy-Library-Items/POLICY_IS2P2.html?DLPage=1&DLEntries=10&DLSort=0&DLSortDir=ascending)
	2. [CMS Acceptable Risk Safeguards (ARS)](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/ARS-31-Publication.html?DLPage=1&DLEntries=10&DLSort=0&DLSortDir=ascending)

## HHS Guidance

1. [HHS Rules of Behavior for Use of HHS Information and IT Resources](https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/hhs-rules-of-behavior-for-the-use-of-hhs-information-and-it-resources-policy.html)
2. [HHS Information Security and Privacy Policy (IS2P)](https://intranet.hhs.gov/technical-support/cybersecurity/policies-standards-memoranda-guides/policies)