HCQIS Data Management Policy for Contractor Furnished Equipment (CFE)

Version 1.1
2/10/2020
Revision/Change Record

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Description</th>
<th>Page, Section Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/02/2019</td>
<td>1.0</td>
<td>Initial Version</td>
<td>All</td>
</tr>
<tr>
<td>02/10/2020</td>
<td>1.1</td>
<td>Updates to various sections (CFE, FISMA, HIPAA Rule, Email guidance, and added FAQ table)</td>
<td>3, 4, 5, 6, 8</td>
</tr>
</tbody>
</table>

Contents

Revision/Change Record ........................................................................................................................................2
Contents ........................................................................................................................................................................2
Introduction ..............................................................................................................................................................3
Contractor Furnished Equipment (CFE) ..................................................................................................................3
FISMA vs. HIPAA ....................................................................................................................................................3
HIPAA Security & Privacy Rule ..........................................................................................................................4
HCQIS CFE and Corporate Email Systems ...........................................................................................................5
Appendix A: Frequently Asked Questions ...........................................................................................................8
Introduction

As an Operating Division of the Department of Health and Human Services (HHS), and the nation’s largest healthcare insurance organization, the Centers for Medicare and Medicaid Services (CMS) is subject to the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule (the Security Rule) & Privacy Rule (the Privacy Rule). While the HIPAA Privacy Rule establishes national standards to protect individuals’ medical records and other personal health information (PHI), the HIPAA Security Rule specifically focuses on the safeguarding of electronic protected health information (ePHI).

Per HIPAA, CMS’ contractors are considered “Business Associates” of CMS and thus are bound by the requirements of the HIPAA Security and Privacy Rules: https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html

Contractor Furnished Equipment (CFE)

Contractor-Furnished Equipment (CFE) consists of items furnished by a contractor for the purpose of performing under a contract, including, but not limited to, hardware, software, commercial items, compliant internet connectivity, and peripherals. Typically, CFE utilizes the Contractors’ “corporate network” and/or resources. Therefore, all provisions of the Security Rule (?) must be implemented to ensure proper safeguarding and data integrity while performing CMS specific tasks.

To access Health Care Quality Information System (HCQIS) internal systems, the Contractor will use the current HCQIS access technology to perform its work upon CMS approval. The Contractor must provide all additional equipment needed to support the requirements of this contract. In doing so, the Contractor and any of its subcontractors must abide by the most recent version of the HCQIS CFE Data Management Policy document and other supporting documents (HCQIS Rules of Behavior, Qualitynet System Security Policy, etc).

FISMA vs. HIPAA

Both the Federal Information Security Modernization Act (FISMA) and HIPAA apply to CMS and its contractors, and include requirements for safeguarding CMS and/or Privacy data during storage, processing, and transmission. CMS characterizes its FISMA systems based on each system’s respective boundaries, as defined by the CMS Program Business Owners (BOs) and Information System Security Officers (ISSOs), using guidance found within the HHS Information Systems Security Policy (IS2P) CMS Information Systems Security and Privacy Policy (IS2P2), and other CMS and federal security policies.

FISMA systems are (in most cases) categorized by the collection of systems and/or application(s) that make-up the boundary identified by the CMS Business Owners and are not necessarily tied to a single network, computer, or database where the data resides. If a contract specifically requires the creation, management, or maintenance of information technology systems/applications or development of data management solutions, then these solutions may require additional safeguarding under FISMA and may require an Authority to Operate (ATO) granted by the CMS Chief Information Officer (CIO). This is usually decided at the time of contract award, but could be required later if dictated by contractual circumstances.
While CMS FISMA systems and data are covered under their respective FISMA boundaries defined in the ATO, that boundary may not cover every operational aspect of the data being managed outside of those CMS boundaries. However, entities are still bound by HIPAA and must comply with the Security and Privacy Rules, the former specifically focusing on protection of the confidentiality, integrity, and availability of ePHI. Any ePHI that a covered entity creates, receives, maintains, or transmits must be protected against reasonably anticipated threats, hazards, impermissible use and/or disclosure.

**HIPAA Security & Privacy Rule**

With CCSQ’s implementation of CFE within the HCQIS environment, organizations may have contractual or operational responsibilities that require Contractors to send and/or receive, or possibly temporarily store CMS data using corporate furnished resources. This may include technologies for storing, processing or transmitting CMS data such as corporate-furnished email, data/file storage, faxing solutions and other technologies. For example, organizations utilizing traditional fax machines will need to physically scan documents onto their corporate network before moving them to the HCQIS network electronically. These CFE resources typically have information technology solutions which include servers, networks, storage and other components that may include elements considered sensitive (Personally Identifiable Information (PII) or PHI) and/or covered under the Privacy Act of 1974.

For organizations looking to utilize their own processes via the new CFE policy, they must ensure that all processes, practices and ANY technical solutions comply with the HIPAA Privacy Rule regulations and the HHS Safeguards for Faxing, ePHI data, for example, must be encrypted during transport, as well as in storage. Contractors are NOT permitted to use cloud-based faxing solutions as there are No FedRAMP-approved solutions at the current time.

The HIPAA Security Rule requires the implementation of certain administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of ePHI. CMS requires any organization handling (storing, processing, and/or transmitting) CMS data in contractor environments to ensure administrative, physical and technical safeguards are in place using the HIPAA Security Rule and the National Institute of Standards and Technology (NIST) Special Publication 800-66 as guidelines for implementing proper, but reasonable, controls. In addition to controls, contractors should follow industry best practices for securing CMS data. This includes, but is not limited to:

- **CMS Program approval** – The CMS Program and Business Owner must approve the solution, which may include recommendations from the ISSO to ensure risk is minimized.

- All Contractors must have a CMS Data Use Agreement (DUA) in place where applicable.

- **Data lifecycle management** – Contractors should, where possible, use CMS systems and resources that hold an ATO for storing CMS data. HCQIS has data/file storage capabilities to allow information to be stored to support business functions, operational support (e.g. backup), as well as long-term/archival needs to help organizations adhere to data retention and records management policies. If CFE is needed for short-term processing of CMS data (process/transmit/store), contractors must limit the amount of data to the minimum required for support of business functions, and operational support. In addition, the number of users with access to that data must be kept to the minimum necessary for the task at hand. Organizations using CFE must minimize the amount of time that data elements reside within the CFE non-ATO’d environments, and ensure that data which is no longer needed is destroyed automatically or manually, as applicable, using acceptable methods. Contractors should also be mindful of potential PII breach events for processes that enable automatic backups.
• **Records Retention** – ALL Contractors are subject to HHS/CMS Records Management policies. However, archiving CMS data within corporate networks is NOT permitted and data should NOT be placed in storage folders that are part of the contractor’s other (non-CMS) business archiving schedule. Contractors must work with their Contracting Officer’s Representative (COR) to determine if utilizing CMS resources would better support records retention needs.

• **Access Controls** – Ensure proper access controls limit information system access to ONLY authorized users, to processes acting on behalf of authorized users, or to devices (including other information systems). Organizations must also limit the types of transactions and functions which authorized users are permitted to conduct to only those necessary to complete the work.

• **Security Best Practices using CFE** – In line with the HCQIS CFE guidelines, ALL CFE operating systems, software, and hardware patch levels must be kept current using the HCQIS patching guide as a reference. In addition, organizations should follow best practices for managing CFE, such as;
  
  o Limit access to information systems, by setting a personal identification number (PIN) or password, and automatically locking a device after an idle period;
  
  o Disable networking capabilities, such as Bluetooth, except when they are needed;
  
  o Use additional security software, such as antivirus software and personal firewalls;
  
  o Ensure that security updates and patches are applied within acceptable timeframes when made available by the vendor; and
  
  o Configure applications to support security (e.g., blocking activity that is likely to be malicious).

• **Use of Encryption** – Contractors must utilize Federal Information Processing Standards (FIPS) 140-2 approved cryptographic algorithms when considering encryption including latest versions of Transport Layer Security (TLS), Secure Socket Layer (SSL), and AES-256 for storage. Contractors should NOT use obsolete versions of these technologies; these are no longer considered secure by federal standards. Any storage media, including laptop hard drives, thumb/flash drives, etc., used for CMS data must be encrypted with a FIPS 140-2 approved product.

• **Personally-owned devices** – Per HHS policy, personally-owned mobile telephones, tablets, and other smart and storage devices shall NOT be used to store and access government sensitive information, unless an exception has been granted and access is managed by an approved enterprise mobile device management (MDM) solution and encryption mechanism. The MDM solution must be configured to the most restrictive settings practicable (in accordance with OpDiv policies) and include separate data containers to segregate HHS information from personal information and allow for remote wipe in the event of an incident involving HHS information.

**HCQIS CFE and Corporate Email Systems**

As CCSQ transitions from GFE to CFE, one of the significant changes is the decommissioning of the HCQIS email system, which served approximately 4,500 users. Although the reasons for offering an “in-house” email solution were sound in a fully GFE environment, migration to contractor provided email provides more flexibility for users while utilizing CFE (e.g., contractor-owned laptops). This section
provides guidance and best practices for securing email transmissions and corporate-managed email systems when communicating with CMS.

**HCQIS Resource Mailboxes and Distribution List:** HCQIS will maintain a limited list of resource mailboxes to support large program or enterprise-level services (e.g. qnetsupport@qualitynet.org). These resource mailboxes have associated costs and are subject to ISG approval. Distribution email addresses are permitted for internal system-to-system communication or may be used to communicate to larger HCQIS Enterprise communities (i.e. no-reply@hcqis.org). Distribution lists may also be subject to ISG approval. All other use-cases may require the Contractor to get a CMS EUA account if a cms.hhs.gov email address is required. Contact your COR for requirements if this is a desired email mailbox.

**HCQIS PST Files:** Contractors using HCQIS Outlook PST (personal storage table) files must have an approved business justification prior to moving any HCQIS email PSTs to their CFE network. Contractors should protect PST files as they would any other CMS data element stored on CFE equipment by assuring the same level of security and privacy provisions listed in the Security and Privacy Rules stated above. Contractors are responsible for creating and transferring their PST file if approved to do so.

**Secure Email Communications** – For email and other communication services, Contractors must adhere to the CMS Acceptable Risk Safeguards (ARS) control: SC-1 System and Communications Protection Policy and Procedures. Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. Contractors should enable TLS on their email systems to reduce risk and improve overall security posture.

In addition to following ARS SC-1 Control, CFE users must comply with the guidance below as they begin using corporate email accounts:

1. Contractors should make all efforts to enforce the latest versions of TLS (at this time, TLS 1.3) encryption on their email systems;
2. Auto-forwarding from HCQIS email to your corporate email account is prohibited. Before “abandoning” your HCQIS email account, it is suggested that an auto-reply message be enabled that provides senders with your new email address (and reminds them to encrypt sensitive data);
3. Avoid emailing sensitive data. When possible, use secure shared storage or secure file transfer systems (i.e. HCQIS MFT, FileCloud, etc), both of which are offered as enterprise services within HCQIS;
4. If you must email sensitive data, encrypt it (utilizing FIPS 140-2 approved encryption) in an attachment to the email and communicate the password out-of-band (i.e. via text or phone);
5. Emails sent automatically from systems that provide status info, error conditions, or other alerts should not contain sensitive information such as host names or IP addresses. This type of email should provide a minimal amount of information, prompting the user to take action if additional information is needed, such as logging into a system to review logs;
6. Saving email attachments to removable media such as flash/thumb drives, USB drives, or recordable CD/DVD media is strictly prohibited. These technologies typically do not employ encryption and their use should be avoided for all CMS data (unless CMS has approved their use and proper encryption is implemented);
7. When deleting HCQIS emails in your corporate email account, please utilize the feature for permanent deletion (i.e.. use **Shift-Delete** in MS Outlook);
8. CMS contract-related emails created and received in your corporate email account must be treated as sensitive and handled accordingly. In addition, National Archives and Records Administration (NARA) data retention requirements do apply to email, so check with your COR to determine how long this data should be retained;

9. Calendar items should not be exported/imported from HCQIS. Please provide your corporate email address to the hosts of any meetings you need or wish to be invited to attend;

10. Email contact information can be exported to a .csv file and imported into your corporate email account. Keep in mind that this could include many hcqis.org email addresses that will no longer be valid;

11. HCQIS-related email business should not be conducted over insecure Wi-Fi access point connections;

12. HCQIS-related email business must not be conducted while traveling outside the United States and its territories;

13. If you believe CMS or HCQIS security policy has been violated and data has potentially been compromised, please contact your organization’s Security Point of Contact (SPOC) or the QualityNet Help Desk at (866) 288-8912 (qnetsupport@hcqis.org) to report a potential security incident.
### Appendix A: Frequently Asked Questions

<table>
<thead>
<tr>
<th>1. Are we authorized to store CMS data on CFE network?</th>
<th><strong>YES.</strong> Authorization is provided via the terms and conditions in your contract, proper Data Use Agreements (DUAs), and permission from the COR, if applicable.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Are we authorized to archive CMS data on CFE network?</td>
<td>At this time, ISG is finalizing the policy of archiving CMS data on CFE for Record Retention compliance. Should you have a need to archive CMS data before the policy is published, please use Amazon Web Services (AWS) S3 (Simple Storage Solution) Glacier, which is available in HCQIS Cloud</td>
</tr>
</tbody>
</table>
| 3. What is considered CMS data? | CMS data is considered to be any data created, used or needed to perform the task within the contract. Data can also be categorized as an official CMS record. You can learn more about records and HHS Records Management here: [https://humancapital.learning.hhs.gov/courses/recordsmanagement/index.html](https://humancapital.learning.hhs.gov/courses/recordsmanagement/index.html)  
  ○ **Note:** Consult with your COR or CMS lead on what specific data is needed for the contract. |
| 4. Can I store PHI/PII on my CFE? | **Yes** – Unless otherwise stated in your DUA or by your COR, you may store sensitive data within your CFE network as long as the proper controls are in place. |
| 5. Is there a limit on how much sensitive data that is stored? | **No** – However, the data management policy states that the Contractor must limit the use of data when applicable by implementing proper Data Management Lifecycles and should also reference the HHS Records Management policy. |
| 6. Wait…I thought I needed a CMS ATO. Will I need an ATO? | **No** – Your CFE systems are not considered a CMS system. Only CMS systems require an ATO and to be FISMA-compliant. |
| 7. Will I ever need to be FISMA compliant or need an ATO? | It depends on the following factors:  
  • FISMA systems are in most cases categorized by the system or application and not by the physical network the data resides. Hence, if your contract requires the management or creation of information technology systems/applications or development of data management solutions, then these solutions may require additional safeguarding under FISMA and will require an Authorization to Operate granted by the CMS Chief Information Officer. |
<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Officer (CIO). This is decided on a case-by-case basis. Contact your COR to obtain a CMS decision.</td>
<td></td>
</tr>
<tr>
<td>• A future change to FISMA policy may require modifications to a system to become FISMA-compliant.</td>
<td></td>
</tr>
<tr>
<td>8. I’m still not clear whether I will need an ATO. What should I do?</td>
<td>• Contact your COR to obtain a CMS decision.</td>
</tr>
<tr>
<td>9. What controls do I need to consider?</td>
<td>• CMS requires all Contractors to be HIPAA- compliant. HIPAA provides guidance within the Security and Privacy Rules.</td>
</tr>
<tr>
<td></td>
<td>• Additional guidance and links to these HIPAA Rules, as well as applicable Federal Security standards, are referenced in the <em>HCQIS Data Management Policy for Contractor Furnished Equipment (CFE)</em>.</td>
</tr>
<tr>
<td>10. How do I comply with the provisions of the Data Management Lifecycles and Retention policies while using CFE?</td>
<td>• While on CFE, you are still bound to comply with CMS Data Management Lifecycle and Record Retention policy.</td>
</tr>
<tr>
<td>11. Can I use my organization’s Corporate Network? If so, what are the requirements?</td>
<td>• Yes, you can use your Corporate network to perform CMS Contract work – as long as you comply with the HCQIS CFE Guidelines and Requirements document. Please note: you may need to perform upgrades to your corporate network assets, including hardware, software, commercial items, IPv6-compliant internet connectivity, and peripherals in order to obtain approval to handle CMS data.</td>
</tr>
</tbody>
</table>