1. HHS FedRAMP Privacy and Security Requirements  
     
   The Contractor (and/or any subcontractor) must be responsible for the following privacy and security requirements:
   1. **FedRAMP Compliant ATO**. Comply with FedRAMP Assessment and Authorization (A&A) requirements and ensure the information system/service under this contract has a valid FedRAMP compliant (approved) authority to operate (ATO) in accordance with Federal Information Processing Standard (FIPS) Publication 199 defined security categorization. If a FedRAMP compliant ATO has not been granted, the Contractor must submit a plan to obtain a FedRAMP compliant ATO by a timeline determined by CMS.
      1. Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline ([www.FedRAMP.gov](http://www.fedramp.gov/)). The *HHS Information Security and Privacy Policy (IS2P),* *HHS Cloud Computing and Federal Risk and Authorization Management Program (FedRAMP) Guidance*, and the CMS Information System Security and Privacy Policy (IS2P2) further define the baseline policies as well as roles and responsibilities. The Contractor must also implement a set of additional controls identified by the agency when applicable.
      2. A security control assessment must be conducted by a FedRAMP third-party assessment organization (3PAO) for the initial ATO and ***annually*** thereafter or whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.
   2. **Data Jurisdiction.** The contractor must store all information within the security authorization boundary, data at rest or data backup, within the Continental United States (CONUS) if so required.  Refer to G.x Contractor Work Performed Outside of the United States and its Territories (April 2016) in the Solicitation/Contract.
   3. **Service Level Agreements.** *Add when applicable* The Contractor must understand the terms of the service agreements that define the legal relationships between cloud customers and cloud providers and work with CMS to develop and maintain an SLA.
   4. **Interconnection Agreements/Memorandum of Agreements.** *Add when applicable* The Contractor must establish and maintain Interconnection Agreements and or Memorandum of Agreements/Understanding in accordance with HHS/CMS policies.
2. Protection of Information in a Cloud Environment
   1. If contractor (and/or any subcontractor) personnel must remove any information from the primary work area, they must protect it to the same extent they would the proprietary data and/or company trade secrets and in accordance with HHS/CMS policies <https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/index.html>.
   2. HHS/CMS will retain unrestricted rights to federal data handled under this contract. Specifically, HHS/CMS retains ownership of any user created/loaded data and applications collected, maintained, used, or operated on behalf of HHS/CMS and hosted on contractor's infrastructure, as well as maintains the right to request full copies of these at any time. If requested, data must be available to HHS/CMS within ***one (1) business day*** from request date or within the timeframe specified otherwise. In addition, the data must be provided at no additional cost to HHS/CMS.
   3. The Contractor (and/or any subcontractor) must ensure that the facilities that house the network infrastructure are physically and logically secure in accordance with FedRAMP requirements and HHS/CMS policies.
   4. The contractor must support a system of records in accordance with NARA-approved records schedule(s) and protection requirements for federal agencies to manage their electronic records in accordance with 36 CFR § 1236.20 & 1236.22 (ref. a), including but not limited to the following:
      1. Maintenance of links between records and metadata, and
      2. Categorization of records to manage retention and disposal, either through transfer of permanent records to NARA or deletion of temporary records in accordance with NARA-approved retention schedules.
   5. The disposition of all HHS/CMS data must be at the written direction of HHS/CMS. This may include documents returned to HHS/CMS control; destroyed; or held as specified until otherwise directed. Items returned to the Government must be hand carried or sent by certified mail to the COR.
      1. If the system involves the design, development, or operation of a system of records on individuals, the Contractor must comply with the Privacy Act requirements*.*
3. Assessment and Authorization (A&A) Process
   1. The Contractor (and/or any subcontractor) must comply with HHS/CMS and FedRAMP requirements as mandated by federal laws, regulations, and HHS/CMS policies, including making available any documentation, physical access, and logical access needed to support the A&A requirement. The level of effort for the A&A is based on the system's FIPS 199 security categorization and HHS*/*CMS security policies. The contractor must obtain authorization prior to deployment or service implementation.
      1. In addition to the FedRAMP compliant ATO, the contractor must complete and maintain an agency A&A package to obtain agency ATO prior to system deployment/service implementation within CFACTS in a timeline to be determined by CMS. The agency ATO must be approved by the CMS authorizing official (AO) prior to implementation of system and/or service being acquired.
      2. CSP systems categorized as Federal Information Processing Standards (FIPS) 199 high must leverage a FedRAMP accredited third-party assessment organization (3PAO); moderate impact CSP systems must make a best effort to use a FedRAMP accredited 3PAO but should not use self-assessment. CSP systems categorized as FIPS 199 low impact may leverage a non-accredited, independent assessor.
      3. For all acquired cloud services, the A&A package must contain the following documentation:
         * Security Assessment Plan (SAP)/Security Assessment Report (SAR)
         * System Security Plan (SSP)
         * Plan of Action and Milestones
         * Contingency Plan and Contingency Plan Test
         * E-Authentication Questionnaire].

Following the initial ATO, the Contractor must review and maintain the ATO in accordance with HHS*/CMS* policies using CMS templates and defined timelines*.*

* 1. HHS/CMS reserves the right to perform penetration testing (pen testing) on all systems operated on behalf of agency. If HHS/CMS exercises this right, the Contractor (and/or any subcontractor) must allow HHS/CMS employees (and/or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with HHS/CMS requirements. Review activities include, but are not limited to, scanning operating systems, web applications, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.
  2. The Contractor must identify any gaps between required FedRAMP Security Control Baseline/Continuous Monitoring controls and the contractor's implementation status as documented in the Security Assessment Report and related Continuous Monitoring artifacts. In addition, the contractor must document and track all gaps for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the risks, HHS/CMS may require remediation at the contractor's expense, before HHS/CMS issues an ATO.
  3. The Contractor (and/or any subcontractor) must mitigate security risks for which they are responsible, including those identified during A&A and continuous monitoring activities. All vulnerabilities and findings must be remediated, in accordance with timelines specified in the HHS POA&M Standard, from discovery: (1) critical vulnerabilities no later than ***fifteen (15) days*** and (2) high within **thirty (30) days** (3) medium within **ninety (90) days** and (4) low vulnerabilities no later ***than three hundred and sixty (360).***In the event a vulnerability or other risk finding cannot be mitigated within the prescribed timelines above, they must be added to the designated POA&M and mitigated within the timelines assigned to the POA&M within CFACTS. HHS/CMS will determine the risk rating of vulnerabilities using FedRAMP baselines.
  4. **Revocation of a Cloud Service**. HHS/CMS have the right to take action in response to the CSP's lack of compliance and/or increased level of risk. In the event the CSP fails to meet HHS/CMS and FedRAMP security and privacy requirements and/or there is an incident involving sensitive information, HHS and/or CMS may suspend or revoke an existing agency ATO (either in part or in whole) and/or cease operations. If an ATO is suspended or revoked in accordance with this provision, the CO and/or COR may direct the CSP to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor information system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

1. Reporting and Continuous Monitoring
   1. Following the initial ATOs, the Contractor (and/or any subcontractor) must perform the minimum ongoing continuous monitoring activities specified below, submit required deliverables by the specified due dates, and meet with the system/service owner and other relevant stakeholders to discuss the ongoing continuous monitoring activities, findings, and other relevant matters. The CSP will work with the agency to schedule ongoing continuous monitoring activities. Meetings shall be held at least monthly, or as needed.
   2. At a minimum, the Contractor must provide the following artifacts/deliverables on a monthly basis via the CCIC requirements which can be provided by contacting [EVM-CMP@cms.hhs.gov](mailto:EVM-CMP@cms.hhs.gov). Deliverables are identified as:
      1. Operating system, database, Web application, and network vulnerability scan results;
      2. Updated POA&Ms;
      3. Any updated authorization package documentation as required by the annual attestation/assessment/review or as requested by the CMS System Owner or AO; and
      4. Any configuration changes to the system and/or system components or CSP's cloud environment, that may impact HHS/CMS security posture. Changes to the configuration of the system, its components, or environment that may impact the security posture of the system under this contract must be approved by the agency.
2. Configuration Baseline
   1. The contractor must certify that applications are fully functional and operate correctly as intended on systems using *HHS Minimum Security Configurations Standards Guidance*. The standard installation, operation, maintenance, updates, and/or patching of software must not alter the configuration settings from the approved HHS*/CMS* configuration baseline.
   2. The contractor must use Security Content Automation Protocol (SCAP) validated tools with configuration baseline scanner capability to certify their products operate correctly with HHS/CMS and NIST defined configurations and do not alter these settings.
3. Incident Reporting  
   1. The Contractor (and/or any subcontractor) must provide an Incident and Breach Response Plan (IRP) in accordance with HHS*/CMS]*, OMB, and US-CERT requirements and obtain approval from CMS. In addition, the Contractor must follow the incident response and US-CERT reporting guidance contained in the FedRAMP Incident Communications.
   2. The Contractor (and/or any subcontractor) must implement a program of inspection to safeguard against threats and hazards to the security, confidentiality, integrity, and availability of federal data, afford HHS/CMS access to its facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of notification. The program of inspection must include, but is not limited to:
      1. Conduct authenticated and unauthenticated operating system/network/database/Web application vulnerability scans. Automated scans can be performed by HHS/CMS personnel, or agents acting on behalf of HHS/CMS*,*using agency-operated equipment and/or specified tools. The Contractor may choose to run its own automated scans or audits, provided the scanning tools and configuration settings are compliant with NIST Security Content Automation Protocol (SCAP) standards and have been approved by the agency. The agency may request the Contractor's scanning results and, at the agency discretion, accept those in lieu of agency performed vulnerability scans.
      2. In the event an incident involving sensitive information occurs, cooperate on all required activities determined by the agency to ensure an effective incident or breach response and provide all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. In addition, the Contractor must follow the agency reporting procedures and document the steps it takes to contain and eradicate the incident, recover from the incident, and provide a post-incident report that includes at a minimum the following:
         * Company and point of contact name;
         * Contract information;
         * Impact classifications/threat vector;
         * Type of information compromised;
         * A summary of lessons learned; and
         * Explanation of the mitigation steps of exploited vulnerabilities to prevent similar incidents in the future.
4. Media Transport
   1. The Contractor and its employees must be accountable and document all activities associated with the transport of government information, devices, and media transported outside controlled areas and/or facilities. These include information stored on digital and non-digital media (e.g., CD-ROM, tapes, etc.), mobile/portable devices (e.g., USB flash drives, external hard drives, and SD cards)*.*
   2. All information, devices and media must be encrypted with HHS/CMS-approved encryption mechanisms to protect the confidentiality, integrity, and availability of all government information transported outside of controlled facilities.
5. Boundary Protection: Trusted Internet Connections (TIC)
   1. The contractor must ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities using cloud services is inspected by Trusted Internet Connection (TIC) processes that are in compliance with the requirements of the Office of Management and Budget (OMB) Memorandum (M) 19-26: Update to the TIC Initiative, TIC 3.0.
   2. The contractor must route all external connections through a TIC.
   3. **Non-Repudiation**. The contractor must provide a system that implements encryption with current FIPS 140 validation certificate from the NIST CMVP that provides for origin authentication, data integrity, and signer non-repudiation.