PERM Contractor Security Measures FAQs

Introduction

Booz Allen Hamilton (Booz Allen) – the Eligibility Review Contractor (ERC), Lewin – the Statistical Contractor (SC), and NCI – the Review Contractor (RC) (collectively "the PERM contractors") are business associates (BAs) of the Department of Health and Human Services (HHS) Centers for Medicare and Medicaid Services (CMS). In addition to CMS-specific security requirements, the PERM contractors also employ internal security requirements to secure all data and information transacted, as well as remote access to information from the states. This document provides questions and answers related to the security requirements, laws, and regulations employed by the Federal Government and CMS, as well as the practices of the PERM contractors.

What Federal Security Requirements do the PERM contractors follow?

As a contractor to CMS, the PERM contractors are subject to the same privacy and security requirements that CMS must follow to ensure the confidentiality, integrity, and availability of CMS information and systems that CMS uses to collect, create, use, disclose, maintain, and store personal, health care, and other sensitive information. Federal security requirements include:

- The Privacy Act of 1974
- Federal Information and Security Modernization Act (FISMA 2014)
- E-Government Act of 2002
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)

In addition to these laws, CMS and its contractors abide by numerous requirements and guidelines published by the Office of Management and Budget (OMB), HHS, National Institute Standard and Technologies (NIST), and CMS-published requirements, including:

- Information Systems Security and Privacy Policy (IS2P2)
- Medicare Program Integrity Manual
- Business Partner System Security Manual (BPSSM)
- Risk Management Handbook (RMH)

CMS Acceptable Risk Safeguards (ARS)

The CMS ARS provide guidance on the minimum acceptable level of required security controls—collectively known as the CMS Minimum Security Requirement (CMSR)—baselines that must be implemented to protect CMS' information and information systems. The CMSR is based on:

- NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013
- Federal Risk and Authorization Management Program (FedRAMP)
- HHS IS2P
- CMS IS2P2 CMS-CIO-POLSEC-2016-0001
- CMS policies, procedures, and guidance
- Other federal and non-federal guidance resources
- Industry leading information security and privacy practices adopted by CMS

What security and privacy training do PERM contractors complete?

To address the laws, regulations, policies, and procedures and protect the sensitive information that is collected, all PERM staff are required to take CMS mandated and also program-specific security and privacy trainings before they are

granted access to project systems, networks, information, and resources. The first training is mandatory training required by all CMS staff with content provided by CMS. Individual contractor-specific training is detailed below. These mandatory trainings reinforce the importance of safeguarding personally identifiable information (PII) and protected health information (PHI), and increases staff awareness of standards and policies to enable them to be engaged and proactive in protecting client data. This training is done annually.

Mandatory CMS Security and Privacy Training

In accordance with the mandates of FISMA and HHS, all CMS employees and contractors with user access to CMS networks, applications, or data must complete mandatory annual Privacy Awareness Training. The training includes knowledge checks after each section.

The training includes the following areas:

- Privacy Specific:
  - Definitions and examples of:
    - PII
    - PHI
    - Control Unclassified Information (CUI)
  - Review of Federal Privacy Requirements and information on everyone's role in safeguarding data
- Information Security Specific:
  - Definitions and examples of threats and vulnerabilities
  - Guidance on use of:
    - Email
    - Passwords
    - PIV cards
    - Tailgating
    - Social engineering
    - Malware
    - Watering holes
    - Phishing
  - Requirements and guidance for securing assets outside the office including:
    - Wi-Fi
    - Traveling
    - Teleworking
  - Requirements and guidance on when and how to report an incident and breach

Mandatory PERM ERC Security and Privacy Training

In addition to the mandatory annual CMS Security and Privacy Training, all PERM ERC staff are required to take additional security and privacy training. This training emphasizes the application of the CMS-required training to PERM ERC's functional activities as well as provides specific PERM ERC training that is unique to the PERM ERC business processes and activities.

All PERM ERC staff are required to abide by and sign an IT Rules of Behavior and a Non-Disclosure Agreement (NDA) prior to accessing the data. All PERM ERC staff are subject to background investigations prior to employment.

The PERM ERC specific training includes:

- PII and PHI definitions as well PERM ERC examples.
- Operational requirements and guidance on:
  - Eligibility case reviews.
  - How to send/receive PII/PHI because the ERC does not allow sensitive PII/PHI to be sent or received by email. All sensitive PII/PHI to be sent/received must be by SFTP, which can be accessed by states (see Section 5.0).
  - The storage (location) and handling procedures for sensitive information.
  - The disposal (archiving or destruction) of sensitive information.
- Specific PERM ERC incident response process to comply with CMS, HIPAA, and state requirements.

Training is refreshed annually with new and refined content to include lessons learned from the previous year.

All PERM ERC staff with significant security and privacy responsibilities are required to complete role-based training accordance with the CMS policy. In addition, team members whose roles that align with the NIST National Initiative for Cybersecurity Education (NICE) framework take additional training based on their role that is aligned with the NICE framework.

Mandatory PERM RC Security and Privacy Training

Upon hire, all PERM RC staff complete CMS Security and Privacy training and an internal Security and Privacy training before gaining access to any systems. All staff repeat the training annually. Internal training focuses on properly handling and protecting PHI/PII along with cybersecurity awareness. If required by the state, the DP review team also completes individual state's security and privacy training before accessing the state's systems.

Mandatory PERM SC Security and Privacy Training

All project team members are required to take the privacy and security training course, "It's Personal-Privacy and Security." The course provides employees with a basic understanding of the importance of securing protected and confidential information and explains company policies, procedures, and practices for securing these data. Security training is held at least every 12 months for existing staff and is administered during the onboarding for new staff.

How do PERM contractors establish data access and use agreements with states?

The PERM contractors work closely with each state to establish contractor-specific data access and/or use agreements to ensure all access and that the use of state data is consistent with state, CMS, and contractor requirements. This process takes place before the beginning of the cycle to confirm that state rules regarding access to information are followed and any additional training for the contractors is completed in a timely manner.

How do PERM contractors send and receive data from the state?

PERM contractors do not allow PHI to be sent via email. All PERM contractors require sensitive PII/PHI data to be sent/received using SFTP, which can be accessed by states and other authorized external users. The SFTP requires multifactor authentication to provide security for transferring sensitive, PII/PHI data. The PERM contractors manage access for external users to the SFTP, and provide support for any issues that arise (password resets, troubleshooting access).

To upload data collected from the states, PERM contractors use FIPS 140.2 validated encrypted USB drives to temporary store the data until it is uploaded to the SFTP site and verified. After successful SFTP transfer, all data from the external drives is securely wiped.

How do PERM contractors store state data?

The ERC only accesses and stores sensitive PII/PHI data in the CMS AWS environment, a secure cloud environment used for engagements requiring the analysis of sensitive data. The PERM ERC received an Authority to Operate (ATO) in September 2020. CMS manages access to this environment, which requires multifactor authentication. The ERC controls access to data within the environment through role-based access on a need-to-know basis. The ERC continuously monitors and logs all access and activity within the CMS AWS environment.

The RC stores PII/PHI in the secure NCI datacenter, collocated in a System and Organizational Controls (SOC) 2 certified datacenter.

The SC transfers sensitive data files that are received by SFTP to our secure SAS server to be processed. The secure SAS server is accessible only to a limited number of team members for the specific project. Other controls include using file-level access control lists, active directory network authentication, strong password management, and anti-virus/malware to minimize vulnerability, enterprise-level firewalls, client VPN, two-form-factor authentication, and Intrusion Detection Systems. Lewin also sends data offsite to a secure storage facility for disaster recovery. Additionally, computer security includes localized firewalls, mandatory password-protection, FIPS compliant hard-disk encryption, and removable media protection.

How will state data be viewed remotely? What privacy and security measures are in place to work remotely?

ERC

The PERM ERC environment is classified as FISMA Moderate. The CMS Acceptable Risk Safeguards (ARS 5.0) define a FISMA Moderate system as having met a level of acceptable risk based on the tolerance of a system's conformity to 261 safeguards. The standards are based on the NIST 800-53 standards and define a system's risk tolerance. NIST publications define and tailor security control baselines. In this model, effective monitoring and enforcement are applied along with continuous documentation using the CMS FISMA Controls Tracking System (CFACTS). This platform provides a common foundation to manage policies, controls, risks, assessments, and deficiencies across the CMS Enterprise.

For the ERC, all data is uploaded into a secure CMS AWS environment that underwent a full independent third-party security assessment against CMS Acceptable Risk Standards and was granted an authority to operate by the CMS CIO in September 2020. Access to the system is only available by VPN using CMS granted credentials and multifactor authentication. The ERC does not allow storing of sensitive PERM data outside of the CMS AWS environment, and transmitting sensitive PII/PHI via email is also not allowed. The CMS AWS environment is continuously monitored both by CMS and the ERC for system and software vulnerabilities, including extensive logging of access, database, and user activity. All ERC staff are required to take annual CMS Security and Privacy Training and specific PERM Security and Privacy Training before being granted access to the system, and annually thereafter. ERC laptops have full disk encryption, but data is not stored on them. Per Federal Government requirements, all sensitive data is encrypted in transit and at rest using AES-256, FIPS 140-2 validated modules.

RC

RC staff may only use RC issued workstations to access the RC information systems or to perform any RC work. Use of personal or non-RC issued computers and/or devices to access the information system is prohibited. RC staff are required to follow all security protocols mandated by the RC and its Federal and State clientele to minimize the risk of security incidents and privacy breaches. RC laptops are protected by endpoint response and protect (ERP) tool that prevents unapproved software from running on the endpoints. Additionally, the RC utilizes endpoint DLP, antivirus, full disk encryption, and endpoints are scanned daily for vulnerabilities.

SC

Network resources are secured and protected using a three-tier architecture, network access control (NAC), file-level access control lists (ACL), network authentication via Active Directory, strong password management, and anti-virus/antimalware scanning. Computer security is maintained via localized firewalls, mandatory password-protected screen savers, FIPS 140-2 compliant hard-disk encryption and removable media protection. The network perimeter is secured and protected using an enterprise-level firewall, client VPN, enterprise-level anti-virus/anti-malware protection, two-form-factor authentication, and intrusion detection systems. Data access is granted only by authorization of the of the data/project owner, which is based on a project-specific access protocol. Requests and approvals are then documented in the SC's enterprise help desk ticketing system as reference. Folders are audited annually to ensure appropriate access. Unauthorized access in not permitted without exclusive access rights being granted. Security updates and anti-virus definitions are automatically deployed to all nodes to minimize risk due to vulnerabilities. Lewin utilizes tapeless disk-based backup solution with data securely replicated to Lewin's disaster recovery site. The SC does not allow storage of any protected data outside of the virtual machine environment.

Will PERM contractors be printing information?

The ERC and SC do not print any information. Printing is possible for the RC although rare, and home office requirements include cross-cut shredders for the destruction of printed materials.

What is the record destruction policy for PERM contractors once PERM records are no longer needed?

PERM contractors adhere to CMS' record retention requirements and upon completion of those requirements will follow the CMS records destruction policy which is compliant with the NIST 800-88 "Guidelines for Media Sanitation" and as defined by Bucket 9 of CMS' Records Schedule, which applies to records in support of compliance and integrity functions.

Security Questions

For questions regarding the ERC's security practices, please contact PERM_ERC@bah.com.

For questions regarding the RC's security practices, please contact PERMRC_2024@empower.ai.

For questions regarding the SC's security practices, please contact PERMSC.2024@lewin.com.