NEW MEXICO
HUMAN SERVICES DEPARTMENT

Medicaid Management Information System Replacement (MMISR) Project

PROPOSAL ADDENDUM 21 (Twenty One)
ADDENDUM TITLE: HHS 2020 Security Operational Guidelines

Created/Updated: January 31, 2018
Version: 1.0

Revision History

Date	Version # and Reason for Revision	Requester	Editor/Author
1/31/2018	1.0 Initial Document	Dan Valdez	Dan Valdez

Security Operational Guidelines

The New Mexico Human Services Department currently has the following controls implemented. The following list of guidelines are provided as a recommended method of implementing the majority of technical, operational, and administrative controls needed to satisfy federal regulatory, compliance standards and requirements.

It is each Contractor's responsibility to ensure that controls are implemented in a manner that satisfies all federal regulatory, compliance standards and requirements.

1) Compliance

Each Contractor must comply with all applicable business, Federal and State security requirements as described in addendum 14 (HHS 2020 Security and Privacy Standards) and adhere to the security standards established by the SI Contractor.

2) SI System Security Plan

Each Contractor must comply with the SI System Security Plan and identify and remediate any changes required in its environment to meet the security requirements of the State, CMS certification and those established by the SI Contractor.

3) Security Plan

Each Contractor must also develop a security plan for its systems based off of the NIST publication 800-18 "NIST Guide for Developing Security Plans for Federal Information Systems".

4) Operational Guidelines

Security is of primary concern to the State as its work affects many lives and the State is required to assure the protection of sensitive or confidential information, of facilities and personnel. Each Contractor must take all necessary steps to ensure that it and its staff are made aware of the security standards that are to be enforced across the framework and within the module. Any hosted environment of each Contractor or its subcontractors is subject to inspection by the State, its agents or Federal partners. No part Solution that holds or handles State data can be hosted off shore.

While performing work under this contract, each Contractor is responsible for the following list of security activities and integrating these activities with the security plan established by the State and SI Contractor.

1. Personnel Screening – consistent with HSD policy, each Contractor must conduct background checks that comply with all applicable State and federal requirements of

staff prior to authorizing access to HSD or other stakeholders' information systems or data including but not limited to IRS Publication 1075, background checks

2. Contractor Personnel Security –in compliance with HSD personnel security requirements, each Contractor must:

   2.1. Require Contractor and subcontractor staff to comply with HSD personnel security policies and procedures;

   2.2. Ensure all Contractor and subcontractor staff complete HSD-provided online security-related training listed below when they join the Project and at least annually thereafter:

      2.2.1. Security Awareness;

      2.2.2. IRS Safeguards;

      2.2.3. Health Insurance Portability and Accountability Act (HIPAA) Training; and

      2.2.4. Privacy Training (for information system Users).

   2.3. Obtain signed individual security training acknowledgements for each Contractor or subcontractor and provide these to the HSD Chief Information Security Officer (CISO) for initial training and for annual re-certifications;

   2.4. Notify HSD within one (1) business day of any personnel transfer or termination of contractor personnel who have HSD credentials or badges, or who have information system privileges;

   2.5. Monitor staff compliance with these security requirements; and

   2.6. If access to State systems is needed, complete a Security Access Request (SAR) form and submit it to the HSD Information Technology Division (ITD) Help Desk.

3. Termination – upon termination of an individual's employment or participation in the Project and consistent with HSD policies and procedures, each Contractor must:

   3.1. Disable information system access for that individual;

   3.2. Terminate or revoke any authenticators or credentials associated with the individual;

   3.3. Submit a Delete All Security Access Request form to the HSD ITD Help Desk;

3.4. Retrieve all security-related HSD information system-related property;

3.5. Assume control of access to HSD information or information systems formerly controlled by the terminated individual;

3.6. Notify the HSD CISO upon termination of the employee; and

3.7. Ensure physical access to HSD and to Contractor facilities is prohibited (e.g., disable badges, change access codes).

4. Rules of Behavior – prior to accessing the HSD network, Contractor's staff must read the HSD Use of State Information Technology Resources Policy and sign and return to the HSD CISO an HSD Information Technology Resource Usage acknowledgement that commits them to comply with HSD policy.

5. Physical Access to Facilities and Computers –each Contractor or subcontractor staff who have access to State or MMISR facilities or computers where confidential information resides, each Contractor must:

5.1. Develop, approve and maintain a list of contractor, subcontractor and State staff with authorized access to the facility;

5.2. Issue and manage authorization credentials for facility access;

5.3. Remove individuals from the facility access list within one (1) business day when access is no longer required;

5.4. Ensure control to Contractor facility ingress and egress by requiring access control systems or guards and verification of access authorization before granting access to the facility;

5.5. Maintain a physical access audit log for visitors to the Contractor facility, including at a minimum the name and date and time of access;

5.6. Ensure that visitors to a Contractor facility are escorted and monitored;

5.7. Secure keys, combinations or other physical access devices associated with the Contractor facility(s);

5.8. Maintain an inventory of physical access devices;

5.9. Change combinations to facilities at least annually and whenever an employee who knows the combination retires, terminates employment, or transfers to another position;

5.10. Change keys when a master key has been lost;

5.11. Ensure that all computers meet HSD security requirements;

5.12. Ensure no facilities hosting State data are located offshore; and

5.13. Ensure that the facilities of any subcontractors meet these same requirements.

6. Remote Access – any remote access to HSD confidential information must be performed using multi-factor authentication. Remote Access is defined as any access to an information system by a User who is communicating through an external network (e.g., the internet). Each Contractor must adhere to HSD and State usage restrictions, configuration and connection requirements and implementation guidance for each type of remote access that is granted only as needed for valid business reasons and subject to CISO approval.

   6.1. Confidential information must not be accessed remotely by Contractor or subcontractor employees, agents, representatives or other staff located offshore.

   6.2. Confidential information must not be received, processed, stored, transmitted or disposed of by any system located offshore.

7. Use of External Information Systems – unless approved by the HSD CISO, each Contractor must prohibit:

   7.1. Access to confidential information from external information systems; and

   7.2. Use of non-HSD-owned information systems, system components or devices to process, store or transmit confidential information;

8. Media – each Contractor must adhere to HSD policy and procedures for:

   8.1. Labeling media containing HSD confidential information to indicate distribution limitations and handling caveats;

   8.2. Physically controlling and securely storing media and protecting media containing HSD confidential information until the media is destroyed or sanitized using State Auditor approved equipment, techniques and procedures;

   8.3. Transporting media:

      8.3.1. Protect and control digital (e.g., diskettes, magnetic tapes, external or removable hard drives, flash or thumb drives, CDs, DVDs) and non-digital (e.g., paper) media during transport outside of controlled areas;

8.3.2. All digital media containing confidential data must be encrypted including when being transported;

8.3.3. Maintain accountability for media containing HSD confidential information during transport outside of controlled areas;

8.3.4. Document activities associated with transport of information system media; use transmittals or equivalent tracking methods to ensure confidential information reaches its intended destination; and

8.3.5. Restrict activities associated with transport of media containing HSD confidential information to involve only authorized personnel.

8.4. Sanitizing media:

8.4.1. Sanitize media containing confidential data prior to disposal, release from control or release for reuse per State Auditor's requirements;

8.4.2. Use sanitization techniques in compliance with applicable Federal and State standards and policies; and

8.4.3. Review, approve, track, document and verify media sanitization and disposal actions in accordance with State Auditor requirements.

9. Email Communications – adhere to HSD and State policy and procedures regarding inclusion of Federal Tax Information (FTI), Protected Health Information (PHI) or Personally Identifiable Information (PII), or other sensitive, confidential or private data within email communications.

10. Improper Inspections or Disclosures – adhere to HSD policy and procedures regarding reporting unauthorized access or disclosure of confidential information. All incidents affecting the compliance, operation, or security of HSD's Confidential Information must be reported to HSD. Each Contractor shall notify HSD of any instances of security or privacy breach issues or non-compliance promptly upon their discovery, but no later than a period of 24 hours. Notification shall include a description of the privacy or security non-compliance issue and corrective action planned and/or taken.