

NEW MEXICO HUMAN SERVICES DEPARTMENT

Medicaid Management Information System Replacement (MMISR) Project



**PROPOSAL ADDENDUM 14 (Fourteen)
ADDENDUM TITLE: HHS 2020 Security, Privacy and Standards**

Created/Updated: January 11, 2017
Version: 1.2

As part of the RFP response, Offeror also must specify how it will comply with the following Security, Privacy and Standards:

- CMS Minimal Acceptable Risk Standards for Exchanges (MARS-E) 2.0 (2015);
- EDIE (Emergency Department Information Exchange) Records System Standards;
- Federal Information Security Management Act (FISMA) of 2002;
- FedRAMP (Federal Risk and Authorization Program) certification. If the vendor and its solution are not FedRAMP certified, the vendor may offer its plan to achieve such certification if applicable;
- Health Information Technology for Economic and Clinical Health (HITECH) Act;
- Health Insurance Portability and Accountability Act (HIPAA) of 1996;
- Internal Revenue Service (IRS) Publication 1075;
- ISO 15408, ISO 27001, ISO 27002, ISO 27003, ISO 27005 and ISO 27034, Information Security;
- New Mexico Administrative Code (NMAC) 1.12.20, Information Security Operation Management;
- NIEM (National Information Exchange Model);
- NIST 800-100, Information Security Handbook: A Guide for Managers (2007);
- NIST SP800-53A R4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations Building Effective Assessment Plans (2014);
- Office of the National Coordinator for Health Information Technology 2017 Interoperability Standards Advisory;
- Payment Card Industry Data Security Standard (PCI DSS);
- Social Security Administration (SSA) Office of Systems Security Operations Management Guidelines;
- State and Federal Security Audits as required, Federal Information Processing Standards (FIPS) 140-2, Security Requirements; and
- State Privacy and Security Policies and Procedures.