ATTACHMENT 8

NEW YORK STATE OF OPPORTUNITY. Department of Civil Service

Non-Material Deviations Template - "Health Maintenance Organizations Specifications for the New York State Health Insurance Program"

Offeror Name: Capital District Physicians' Health Plan, Inc.

An Offeror is required to use this Non-Material Deviations Template when submitting any proposed non-material deviations and/or alternates. Offeror's proposed deviations must be submitted with its Proposal. Each proposed deviation (addition, deletion, counter-offer or modification) must be specifically enumerated, in a writing, which is not part of a pre-printed form. The writing must identify the specific Solicitation requirement (if any) the Offeror rejects or proposes to modify by inclusion of deviation. The Offeror must enumerate the proposed deviation (addition, deletion, counter-offer or modification) from the Solicitation, and the reasons. **Note**: Every column of the template must be completed.

Deviation Number	Page #	Section Reference	Proposed Deviation with Detailed Explanation
1		Appendix C, 4.2	CDPHP has a SOC2 type 2 certification. Annually CDPHP undergoes a SOC 2 Type 2 audit conducted by an independent audit firm. CDPHP's SOC2 type2 does covers the IT Security Policies noted at https://its.ny.gov/ciso/policies/security. CDPHP reviewed these policies to ensure coverage in our SOC 2 and compliance. Our SOC 2 Type 2 audit covers more than HITRUST, through the inclusion of the Security, Confidentiality, Availability and Privacy Trust Services categories. The SOC 2 Type 2 audit is extensive and addresses the following control areas: communication and information; risk assessment; monitoring activities; control activities; logical and physical access controls; system operations; change management; risk mitigation; and the additional criteria for availability; confidentiality; and privacy. CDPHP is planning to further enhance the SOC 2 Type 2 audit by performing an assessment for the trust principle of processing. CDPHP believes a SOC2 Type 2 is the appropriate certification and it is required by several clients. CDPHP is asking for an alternative to the HITRUST report requirement with a SOC 2 Type 2 audit report.
2		Appendix C, 8.5	CDPHP does have the capability to produce de-identified data for testing as needed but CDPHP would like to deviate from the requirement to use de-identified confidential data in non-production environments. We apply stringent controls on our non-production environments that mirror our production environment (both on premise and cloud), including but not limited to: * Role based access is administered by Access & Identity Management team * 24x7 monitoring and logging * Data Loss Protection (DLP) monitoring CDPHP would like to deviate from the requirement prohibiting the placement of confidential data in a cloud test environment. CDPHP has a dedicated AWS Test Environment with the following compensating controls:

			* CDPHP applies the same level of preventative and detective security controls to our AWS test environment as we do for our AWS production environment. *CDPHP AWS environments are configured and managed internally by CDPHP. * Use of Amazon Configuration tool to ensure environments are stood up with secure configuration to function as a CASB. * Encryption at rest and in-transit is enforced and it is FIPS 140-2. * Role based access is maintained in all environments. * 24x7 monitoring and logging * Data Loss Protection (DLP) monitoring CDPHP is performing an assessment to implement data de-identification/masking across all environments while maintaining our ability to perform comprehensive testing of all permutations as if we are using live data.
3		Appendix C, 15	CDPHP does not allow access from offshore. CDPHP allows trusted offshore partners to view data after appropriate vendor vetting is performed and with periodic re-assessment. *CDPHP uses offshore resources which are limited to view capabilities of data residing in CONUS on CDPHP owned and managed systems. This data cannot be copied, printed, stored or modified outside CDPHP facilities. *CDPHP requires partners to comply with HIPAA/HITECH and NYS regulations including all administrative, physical and technical security controls including but not limited to business, privacy and security training, background checks, and encryption. * Offshore resources are subject to the same new employee training, security awareness, phish testing and annual compliance training as required for all CDPHP employees. *Offshore resources are physically separated from other clients at the offshore facility in "clean" CDPHP rooms. Offshore resources working on the CDPHP account are the only offshore people allowed entry to CDPHP rooms. The doors are locked with entry via authorized access badges. The rooms also have camera coverage throughout the rooms to ensure proper protocols are followed by offshore resources. *Annually CDPHP engages an independent 3rd party to audit and assess offshore facilities and controls. The audit is conducted physically onsite at the offshore location. The audit includes testing of controls similar to a SOC2 Type 2 or HITRUST. We may target areas based on risk or current topics in the news. The independent 3rd party conducts the audit on the behalf of the CDPHP CISO and results are reported directly to the Audit Committee of the Board of Directors and Executive management. The 3rd party also provides services related to the general operating environment and cultural situations that CDPHP needs to be alert to i.e. weather, national celebrations etc. * Also CDPHP adheres to CMS requirements relating to use of offshore resources including informing CMS prior to usage of offshore resources. If the state wishes for CDPHP to eliminate the ability for offshore resources to view data, CDPHP would do that.